NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

DATA CENTRIC INTEGRATION AND ANALYSIS OF INFORMATION TECHNOLOGY ARCHITECTURES

by

Kristin Giammarco

September 2007

Thesis Co-Advisors: Gary Langford
John Osmundson

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704-0188*
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** September 2007	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE: Data Centric Integration and Analysis of Information Technology Architectures			**5. FUNDING NUMBERS**
6. AUTHOR(S) Kristin Giammarco			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

The premise of this thesis is that integrated architectures have increased usefulness to the users of the systems they describe when they can be interactively and dynamically updated and used in conjunction with systems engineering analyses to enable systems optimization. In order to explore this premise, three research topics are presented. The first topic discusses needs and uses for integrated architectures indicated throughout Department of Defense (DoD) policies, directives, instructions, and guides. The second topic presents a systems engineering analysis process and discusses the relevancy of integrated architectures to these analyses. Building on the previous two topics, the third discusses federation, governance, and net-centric concepts that can be used to significantly improve DoD Enterprise Architecture development, integration, and analysis; with specific recommendations for the Army Architecture Integration Process. A key recommendation is the implementation of a collaborative environment for net-centric architecture integration and analysis to provide a rich and agile data foundation for systems engineering and System of Systems engineering analyses, which are required to optimize the DoD Enterprise Architecture as a whole. Other conclusions, recommendations, and areas for future work are also presented.

14. SUBJECT TERMS Systems Engineering Analysis, DoD Enterprise Architecture, System of Systems, Integrated Architecture, DoDAF, Architecture Federation, Governance Architecture, Net-Centric Environment, Modeling & Simulation, Architecture Agility, Authoritative Reference Data			**15. NUMBER OF PAGES** 179
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89) Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

DATA CENTRIC INTEGRATION AND ANALYSIS OF INFORMATION TECHNOLOGY ARCHITECTURES

Kristin Giammarco
DB-03, United States Army
B.E., Stevens Institute of Technology, 1999

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN SYSTEMS ENGINEERING MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
September 2007

Author: Kristin Giammarco

Approved by: Prof. Gary Langford
Thesis Co-Advisor

Dr. John Osmundson
Thesis Co-Advisor

Dr. David H. Olwell
Chair, Systems Engineering Department

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The premise of this thesis is that integrated architectures have increased usefulness to the users of the systems they describe when they can be interactively and dynamically updated and used in conjunction with systems engineering analyses to enable systems optimization. In order to explore this premise, three research topics are presented. The first topic discusses needs and uses for integrated architectures indicated throughout Department of Defense (DoD) policies, directives, instructions, and guides. The second topic presents a systems engineering analysis process and discusses the relevancy of integrated architectures to these analyses. Building on the previous two topics, the third discusses federation, governance, and net-centric concepts that can be used to significantly improve DoD Enterprise Architecture development, integration, and analysis; with specific recommendations for the Army Architecture Integration Process. A key recommendation is the implementation of a collaborative environment for net-centric architecture integration and analysis, to provide a rich and agile data foundation for systems engineering and System of Systems engineering analyses, which are required to optimize the DoD Enterprise Architecture as a whole. Other conclusions, recommendations, and areas for future work are also presented.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS

Acronym	Definition
AAIC	Army Architecture Integration Center
AAIP	Army Architecture Integration Process
AAR	After Action Review
AIP	Architecture Interoperability Program
ASEO	Army Systems Engineering Office
AV	All View
BEA	Business Enterprise Architecture
BMA	Business Mission Area
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, Reconnaissance
CADM	Core Architecture Data Model
CBA	Capabilities-Based Analysis
CDD	Capability Development Document
CIO/G-6	Army Chief Information Officer
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CJCSM	Chairman of the Joint Chiefs of Staff Manual
COA	Course of Action
CoC	Council of Colonels
CPD	Capability Production Document
DAG	Defense Acquisition Guidebook

Acronym	Definition
DARS	DoD Architecture Registry System
DAS	Defense Acquisition System
DAU	Defense Acquisition University
DBSMC	Defense Business Systems Management Committee
DISR	DoD IT Standards Registry
DoD	Department of Defense
DoDAF	DoD Architecture Framework
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
DSS	Decision Support System
DTIC	Defense Technical Information Center
EA	Enterprise Architecture
EEA	Essential Elements of Analysis
FoS	Family of Systems
GAO	Government Accountability Office
GIG	Global Information Grid
HSI	Human Systems Integration
HWIL	Hardware in the Loop
IED	Improvised Explosive Device
IEEE	Institute of Electrical and Electronics Engineers
INCOSE	International Council On Systems Engineering
IP	Internet Protocol

Acronym	Definition
IPL	Integrated Priority List
IPR	Interim Progress Review
IPT	Integrated Product Team
ISP	Information Support Plan
IT	Information Technology
JCIDS	Joint Capabilities Integration and Development System
JROC	Joint Requirements Oversight Council
JUON	Joint Urgent Operational Need
KIP	Key Interface Profile
KPP	Key Performance Parameter
KSA	Key System Attribute
LP	Linear Program
M&S	Modeling & Simulation
MOE	Measure of Effectiveness
MOP	Measure of Performance
MOS	Measure of Suitability
NCDS	Net-Centric Data Strategy
NCE	Net-Centric Environment
NCOW RM	Net-Centric Operations and Warfare Reference Model
NCW	Net-Centric Warfare
NSS	National Security Systems
OA	Operational Architecture

Acronym	Definition
OHIO	Only Handle Information Once
OMB	Office of Management and Budget
OR	Operations Research
OSD(NII)	Office of the Secretary of Defense Networks and Information Integration
OV	Operational View
PEO	Program Executive Officer
PfM	Portfolio Management
POC	Point of Contact
PPBE	Planning, Programming, Budgeting, and Execution
SA	Systems Architecture
SE	Systems Engineering
SEP	Systems Engineering Plan
SOP	Standing Operating Procedures
SoS	System of Systems
SoSE	System of Systems Engineering
SV	Systems and Services View
SWIL	Software in the Loop
T&E	Test & Evaluation
TA	Technical Architecture
TEMP	Test & Evaluation Master Plan
TTV	Target Technical View

Acronym	Definition
TV	Technical Standards View
UJTL	Universal Joint Task List
USD (AT&L)	Under Secretary of Defense Acquisition, Technology & Logistics
V&V	Verification & Validation
WMA	Warfighter Mission Area
XML	eXtensible Markup Language

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

This thesis explores the premise that integrated architectures have increased usefulness to the users of the systems they describe when they can be interactively and dynamically updated and used in conjunction with systems engineering analyses to enable systems optimization. It investigates references to integrated architectures throughout Department of Defense (DoD) policies and guides, describes uses and decision making processes that integrated architectures support, and suggests how integrated architectures can more effectively support these decision making processes by implementing key concepts found throughout DoD policy, using the Army Architecture Integration Process (AAIP) as a point of reference. The term *users* in the premise statement includes warfighters (soldiers, sailors, marines, and airmen in theaters of operation) as well as individuals operating the systems at the enterprise level who support the warfighters, including decision makers.

The fundamental assumption underlying the premise is that architectures may serve a purpose beyond initial design aid, documentation, and major decision point check-the-block requirements; and become a dynamic data foundation upon which analyses are conducted to continuously improve the design and provide rigor behind acquisition and deployment decisions.

In order to explore the premise, three research questions are investigated, corresponding with the subjects of Chapters II, III and IV, respectively. The results of the investigation are detailed in Chapter V, and briefly summarized below.

What do DoD policy and guidance state about the need for integrated architectures? The information provided in Chapter II discusses in detail the needs for and directives to develop integrated architectures in DoD, the architecture framework used for relating architectural data, features, and characteristics of integrated architectures, and various uses for integrated architectures referenced throughout the literature. In addition to being mandated by federal law, architectures serve “to support strategic planning, transformation, and various types of analyses (i.e., gap, impact, risk) and the decisions made during each of those processes” (Volume I, Section 3.1, DoDAF, 2007). The takeaway from the detailed description of the uses of integrated architectures provided in Chapter II is that the ultimate purpose of architecture data is to inform decision-supporting analyses, which are aimed at improving the system described in the architecture, in an iterative way, throughout its entire lifecycle.

How do integrated architectures support systems engineering analysis? The information provided in Chapter III documents the quick reaction process used by the Army Systems Engineering Office (ASEO) to conduct systems engineering, and identifies existing correlations between this process and the DoDAF six-step architecture development process. Chapter III also describes how integrated architectures are used in the context of a systems engineering analysis process, and how that process may be applied to the Joint Capabilities Integration and Development System (JCIDS) process and Defense Acquisition Process. A major finding is that the systems engineering analysis process and the Department of Defense Architecture Framework (DoDAF) architecture development process should be brought together into one process so that integrated architectures become the source data used to conduct systems engineering analyses, and in turn, the systems engineering analysis results and conclusions are applied directly to the improvement of these integrated architectures to deliver higher quality products to the warfighter.

How could the architecture development and integration process be improved to better support systems engineering analysis needs? In order to give a relevant context to this analysis, Chapter IV summarizes and evaluates the Army Architecture Integration Process (AAIP) for potential improvements based on three concepts: architecture federation, governance architecture, and net-centric operations and warfare. The recommendations resulting from this chapter are based on research conducted for and documented in Chapters II through IV. Although the process that was analyzed in detail is Army-specific, the recommendations for the AAIP as it evolves are applicable in any program, component, mission area or enterprise-level context. The recommendations based on the research are aimed to enable large-scale, collaborative, high fidelity systems engineering analysis of integrated architectures. The information in Chapter IV can be used to define the design criteria for a net-centric architecture integration environment that can be used by the Army and other DoD components to integrate, analyze and optimize their architectures in the context of the overall DoD Enterprise Architecture.

In order to truly prove the premise as it is phrased, one needs to test it by developing an integrated architecture and providing its users with an environment in which they can interact with the data and dynamically update it, and assess the usefulness of the architecture in conjunction with systems engineering analyses and systems optimization. Although the research did not include the construction of such an experiment, the research found much evidence to support the premise throughout policies, guides, and processes. Additional conclusions, recommendations, and suggestions for future work regarding the thesis premise are detailed in Chapter V.

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to extend my gratitude to those who supported me in my completion of this thesis and the PD21 program. First, I would like to thank the excellent Naval Postgraduate School instructors and staff, who really brought the course material to life. They made the lessons so practical and relevant that my command, my office and my sponsor were able to benefit from them throughout the program. Special thanks to my thesis advisors, Prof. Gary Langford and Dr. John Osmundson, for the very helpful feedback and guidance throughout the program and on this thesis. Special thanks also go to Dr. Walter Owen and Dr. Benjamin Roberts for making the distance learning and industry trip experiences so effective. Very special thanks go to my cohorts, who have collaborated with me throughout the program and from whom I have learned a very great deal, especially WindyJoy Majumdar, Debbie Clark, and Ronald Clemens. Though geographically dispersed, we worked nearly as easily and frequently as if we were just down the hall from one another. Thank you, sincerely, for always being there, and for going the extra mile (or twelve hundred).

I would also like to recognize and thank those who have contributed to my educational experience at NPS closer to home. Very special thanks to Monica Farah-Stapleton, for sponsoring my application to PD21, for tolerating my Friday absences from the office in the first year, and for encouraging me to keep at it throughout the program. Very special thanks also go to Norma Kornwebel, for continuously encouraging me, for tolerating my Friday absences from the office in the second year, and for supporting me when I needed to take time off to work on my thesis. Special thanks go to Gregory Lorenzo and Lemuel Cline, for enabling and facilitating activities essential to my distance education – you have made all the difference. Thank you also to all those who have provided feedback and suggestions for improving draft chapters, especially LTC Cliff Daus, Bruce

Warrington, and Dr. Deepinder Sidhu. Finally, and most importantly, my sincere thanks go to my family, for sharing me with my schoolwork over the past two years, and for their tremendous support during a very demanding period of time.

I. INTRODUCTION

A. PURPOSE

The purpose of this thesis is to explore the premise that integrated architectures have increased usefulness to the users of the systems they describe when they can be interactively and dynamically updated and used in conjunction with systems engineering analyses to enable systems optimization. This thesis investigates references to integrated architectures throughout Department of Defense (DoD) policies and guides, describes uses and decision making processes that integrated architectures support, and suggests how integrated architectures can more effectively support these decision making processes by implementing key concepts found throughout DoD policy, using the Army Architecture Integration Process (AAIP) as a point of reference. The term *users* in the premise statement includes warfighters (soldiers, sailors, marines, and airmen in theaters of operation) as well as individuals operating the systems at the enterprise level who support the warfighters, including decision makers.

The fundamental assumption underlying the premise is that architectures may serve a purpose beyond initial design aid, documentation, and major decision point check-the-block requirements; and become a dynamic data foundation upon which analyses are conducted to continuously improve the design and provide rigor behind acquisition and deployment decisions.

B. BACKGROUND

The term *architecture* is defined in the Department of Defense Architecture Framework (DoDAF) version 1.5 as “the structure of components, their relationships, and the principles and guidelines governing their design and evolution over time” (p. xiv, Volume II, DoDAF, 2007). The term *integrated architecture* is defined in the same document as “one in which architecture data elements are uniquely identified and consistently used across all products and views within the architecture.” An architecture is said to be integrated when “products and their constituent architecture data elements are developed, such that architecture data elements defined in one view are the same (i.e., same names, definitions, and values) as architecture data elements referenced in another view” (p. 2-1). The Joint Capabilities Integration and Development System (JCIDS) instruction defines an integrated architecture as “an architecture consisting of multiple views or perspectives (operational view, systems view, and technical standards view) that facilitates integration and promotes interoperability across capabilities and among related integrated architectures” (p. GL-9, CJCSI 3170.01F, 2007). The Acquisition Modeling & Simulation Master Plan (DoD M&S Master Plan, 2006) builds on this definition by defining an integrated architecture as “An architecture consisting of multiple views or perspectives (operational view, systems view, technical standards view) that facilitates integration, promotes interoperability, and permits identification and prioritization of capability shortfalls and redundancies.” Unlike the previous definitions, this last definition concludes with a reference to a purpose for and use of integrated architectures.

Development, maintenance, and implementation of integrated Information Technology (IT) architectures are mandated by federal law (Clinger-Cohen Act, 1996; Title 40, Section 1425, 2002; and Title 40, Subtitle III, 2005). Chief Information Officers (CIOs) of all executive agencies facilitate their respective integrated IT architecture development. An *IT Architecture* is defined in the Net-Centric Operations and Warfare Reference Model (NCOW RM) as “an integrated framework for evolving or maintaining existing information technology and acquiring new information technology to achieve the agency's strategic goals and information resources management goals” (Para. 2.1, Introduction, NCOW RM). An IT architecture may be referred to as an *Enterprise Architecture* when it is “the explicit description and documentation of the current and desired relationships among business and management processes and information technology” (Para. 2.1, Introduction, NCOW RM, 2005). The enterprise architecture describes both a "current architecture" and a “target architecture,” and includes a strategy for transitioning from the current environment to the target environment. The enterprise architecture of the Department of Defense is the Global Information Grid (GIG) Architecture. The GIG Architecture Version 1 describes DoD's current IT capabilities and environment, and the GIG Architecture Version 2 describes its target net-centric IT capabilities and environment. The NCOW Reference Model describes DoD's means, mechanisms and strategies for transitioning from Version 1 to Version 2 (Para. 2.1, Introduction, NCOW RM, 2005).

There are a multitude of challenges associated with developing integrated architectures that can be used for the purposes described in the following chapters. The first challenge is in understanding the requirements for an architecture, what problem or problems it will be built to solve, and ensuring the development of the right architecture products to capture the information necessary to address the problem. Another challenge is developing the architecture so that the constituent products are complete and consistent with one another, and verifying consistency, data quality and compliance with architecture standards such as the Department of Defense Architecture Framework (DoDAF) and the Core Architecture Data Model (CADM). Once the robustness of the architecture data is verified, the next challenge must be confronted: that of assessing, improving and optimizing the architecture. These types of analyses involve predicting the performance of the architecture, reducing risk in transformation and modernization using the architecture, and using the analysis results to develop survivable (i.e., the ability to provide reduced services with approximately $^{2}/_{3}$ of network resources down), self-healing (i.e., the ability to be restored without human intervention) architectures and to predict emergent properties of the architecture. These challenges are compounded when developing an architecture for a System of Systems.

There are no globally accepted definitions for *System* and *System of Systems* (SoS); the following definitions for each term are a sampling from multiple sources:

System:

- “A combination of interacting elements organized to achieve one or more stated purposes.” (p. Appendix 8 of 14, INCOSE Systems Engineering Handbook version 3, 2006)
- “A whole that cannot be divided into independent parts without losing its essential characteristics as a whole.” (p. 46, Guide to SoSE, 2006)

System of Systems (SoS):

- “An interoperating collection of component systems that produce results unachievable by the individual systems alone.” (p. 2.2 of 10, INCOSE Systems Engineering Handbook version 3, 2006)
- “A set or arrangement of systems that results when independent and useful systems are integrated into a larger system that delivers unique capabilities.” (p. 8, Guide to SoSE, 2006)
- “A set or arrangement of interdependent systems that are related or connected to provide a given capability. The loss of any part of the system could significantly degrade the performance or capabilities of the whole. The development of an SoS solution will involve trade space between the systems as well as within an individual system performance.” (p. GL-19, CJCSI 3170.01F, 2007 and Section 4.2.6, DAG, 2006)

A more complete literature survey on definitions is provided in Appendix 2, pp. 48-55 in (Guide to SoSE, 2006). For the purpose of this thesis, the last definition of SoS given above provides the most comprehensive description, since the premise involves analysis of performance tradeoffs (among other things) using architectures. The DoD Enterprise Architecture (the GIG) can be considered a System of Systems consisting of components and programs. The components and programs can be considered individual systems that, in turn, consist of sub-systems. This hierarchy is further discussed in Chapter II.

Given the above definition of SoS, the connection between integrated architectures and systems / SoS is presented here in the context and scope of this thesis. In DoD, warfighters depend on IT systems to supply the command and control, communications, and intelligence information needed to successfully complete their missions, maintain information superiority and operate well within an enemy’s decision cycle to ensure his decisive defeat. To enable timely and reliable dissemination of this information from those who have it to those who need it, the individual systems must work efficiently together as an SoS. SoS engineering analyses are conducted to assess the technical performance and capabilities of systems operating in an SoS construct in order to detect and remedy problems before they emerge in a deployed operational environment. These analyses result in recommendations for design corrections, enhancements and integration of new capabilities into current and future forces while ensuring a smooth migration from the “as is” state to the “to be” state. These recommendations are used to inform acquisition and deployment decisions concerning systems and SoS, requiring traceability to a credible set of data. The thesis premise pertains to the use of integrated architectures as this set of data to inform such decisions through rigorous, dynamic analyses conducted on the integrated architecture.

Though this thesis is written in terms to enable maximum applicability and cross-leveraging within DoD and other joint, global enterprises, the impetus for this thesis is current work being performed by the Office of the Army Chief Information Officer (CIO/G-6) Army Architecture Integration Center (AAIC) to improve the architecture development and integration process for the Army. To provide perspective on the uses for integrated architectures and the premise for implementing architecture integration in the highly dynamic, net-centric fashion discussed in this thesis, the most current draft of the Army Integrated Architecture Development Process (Figure 1) is used as a baseline. The process describes all of the steps necessary to develop an integrated architecture, but does not yet detail how to perform ongoing integration, updates and maintenance of architectures in a net-centric manner after the “End.” The above missing piece of the process (which is still in the draft stage and undergoing improvements within the community) serves as the problem statement addressed by the premise.

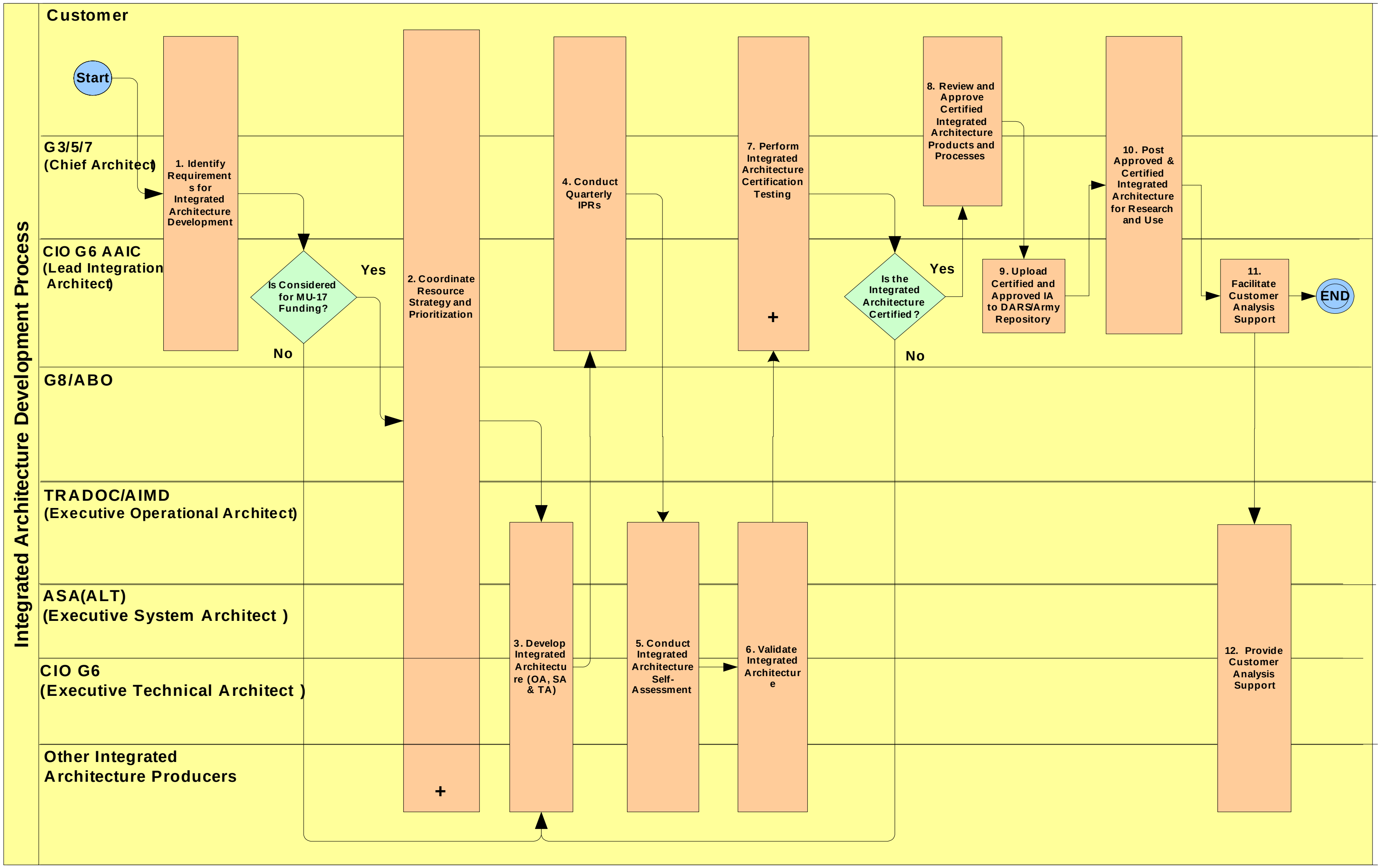


Figure 1 Integrated Architecture Development Process (Main Process) (From: Annex - A, Figure 1, Army CIO/G6 AAIC, 2007)

C. RESEARCH QUESTIONS

The research questions described in this section were developed to provide focus areas for the thesis and to shape the research and subsequent analysis of the data and information collected. The three research questions below correspond with the subjects of Chapters II, III and IV, respectively. The methodology presented in Section F is used to address the research questions. The results and conclusions on the research questions and on the thesis premise are summarized in Chapter V.

1. What do DoD Policy and Guidance State about the Need for Integrated Architectures?

This research reviews DoD policies, directives, instructions, manuals and guides for pertinence to integrated architectures and extracts highlights of guidance on their purpose and use.

2. How do Integrated Architectures Support Systems Engineering Analysis?

This research documents a systems engineering analysis process used by the Army Systems Engineering Office (ASEO), which has roots in DoD, industry and academic publications. The relevance of integrated architectures to this process is explored.

3. How Could the Architecture Development and Integration Process be Improved to Better Support Systems Engineering Analysis Needs?

This research investigates potential architecture development and integration process improvements in the context of net-centric operations and warfare, with the objective of facilitating large-scale, high fidelity systems engineering analysis of the integrated architecture.

D. SCOPE

The research is scoped to IT integrated architecture development efforts within DoD, with a focus on Army processes. However, many of the processes and techniques discussed are applicable to complex architecture integration and analysis efforts in any joint, global organization.

E. BENEFITS OF STUDY

DoD requires a timely, persistent, proactive and reactive architecture integration and analysis environment to deliver capabilities from the enterprise level down to the warfighter. The potential net-centric improvements to the architecture integration process supports accurate and effective portfolio management (PfM), acquisition program and quick reaction analysis requirements, and optimization of systems and SoS. This research will directly benefit the CIO/G-6 AAIC by supporting its mission as the Lead Integration Architect for the Army, and indirectly benefit developers of all SoS architectures through the findings and conclusions that are useful to all joint, global organizations that use integrated architectures in defining IT operations in their enterprise.

This thesis also serves as a reference document for use by architects and systems engineers of joint, global organizations for:

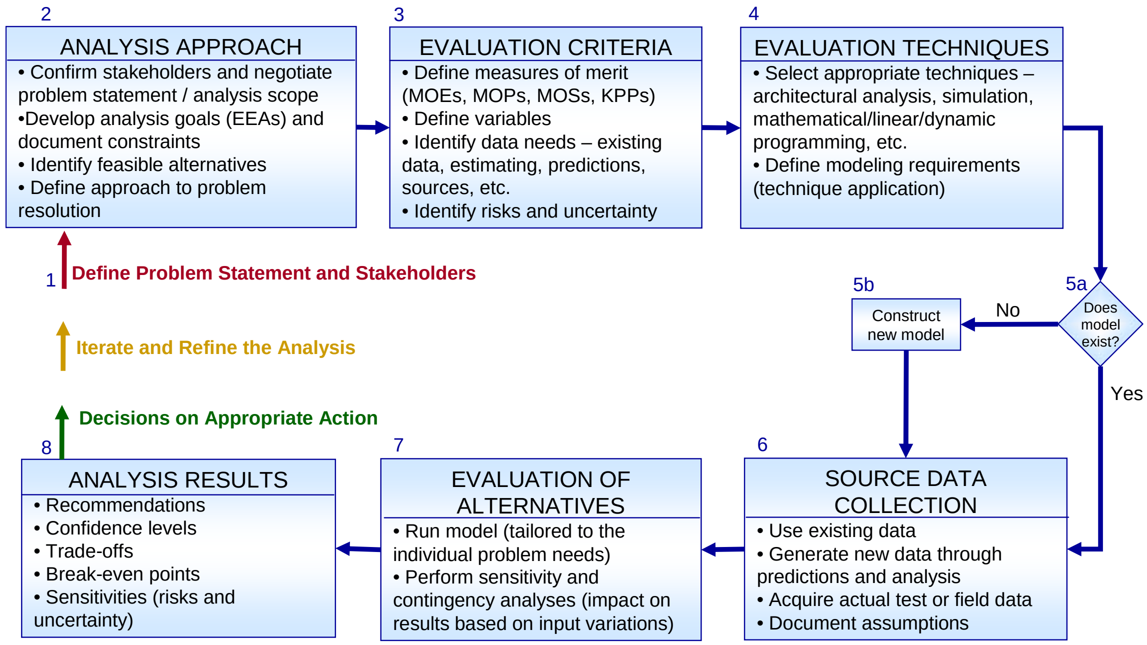
- obtaining a digest of references to integrated architectures in DoD policy and guidance,
- comparing and contrasting their own systems engineering analysis processes with the process documented herein, and
- gaining ideas on how to improve their analysis processes and methods for conducting architecture integration in a net-centric fashion.

This thesis is a beneficial resource to senior engineers, architects and leaders in need of a consolidated reference on the uses and employment of integrated architectures in a net-centric environment, as well as to new engineers and architects who require an introduction to the same.

F. METHODOLOGY

The premise of this thesis is explored via the three interrelated research questions presented earlier, which are organized in Chapters II through IV of this thesis, respectively. Chapter II discusses needs and uses for integrated architectures indicated throughout DoD policies, directives, instructions and guides. Chapter III discusses a systems engineering analysis process used by the ASEO to address questions about systems consistent with the policies in Chapter II, and the relevancy of integrated architectures to these analyses. Building on the needs and uses for integrated architectures established in the previous two chapters, Chapter IV discusses concepts and makes recommendations for meeting architecture needs via an environment for net-centric architecture integration and analysis that is compliant with the Net-Centric Operations and Warfare Reference Model (NCOW RM), enabling rigorous analyses to dynamically and iteratively be conducted on the integrated architecture. Chapter V presents thesis conclusions, summarizes recommendations, and outlines areas for future work.

The methodology used to develop this thesis is a systems engineering analysis process in and of itself. The step-by-step methodology used as a guide for developing this thesis is illustrated in Figure 2. For a full definition and description of the process steps, refer to Chapter III. Below, a customized thesis research methodology is described in the context of this systems engineering analysis process. Sub-steps in the figure that are not applicable to the customized methodology have been omitted.



* Adapted by US Army RDECOM CERDEC ASEO from Figure 4.9 (p. 112) in Blanchard & Fabrycky, "Systems Engineering and Analysis", Fourth Edition, Pearson Prentice Hall, Copyright 2006

Figure 2 ASEO Systems Engineering Analysis Process

1. Define Problem Statement(s) and Stakeholders for Thesis Coordination

The problem statement addressed by this thesis is that the Army Integrated Architecture Development Process describes all of the high-level steps necessary to develop an integrated architecture, but does not yet detail how to perform ongoing integration, updates and maintenance of architectures in a net-centric manner after the "End" of the process in Figure 1. Organizations with which this thesis has been coordinated are as follows:

- Naval Postgraduate School (NPS)
- Army Systems Engineering Office (ASEO)
- CIO/G-6 Army Architecture Integration Center (AAIC)

2. Analysis Approach

A premise was defined to guide the exploration of the problem: Integrated architectures have increased usefulness to the users of the systems they describe when they can be interactively and dynamically updated and used in conjunction with systems engineering analyses to enable systems optimization. It is assumed that such efficiency in updating architectures is both technically feasible and desirable.

Develop Essential Elements of Analysis (EEAs) and constraints. In the case of this thesis, the EEAs are the research questions and the constraint on the analysis is the thesis scope, all of which were discussed earlier in this chapter. Another constraint was time, since this thesis was schedule-driven.

Identify premise or feasible alternatives. The analysis conducted in this thesis centered on determining the validity of the premise rather than identifying feasible alternatives.

Define approach to problem resolution. The general approach for this thesis was the customized version of the systems engineering analysis process presented in Chapter III that is discussed herein. The research questions were addressed by conducting a literature review and synthesis as opposed to a quantitative analysis. The results of the literature review are structured by subject across three chapters as described earlier, and results and recommendations pertaining to the relevant research questions are addressed in the appropriate chapters.

3. Evaluation Criteria

Identify data needs. This step determined the information and data that is needed to address the research questions. Publications that discuss integrated architectures, DoD policies and guidance, and reference models were required for this thesis. Publications were scanned for existing research in the area of the EEAs defined in this thesis in order to determine whether these questions have already been addressed. Potential information and data sources initially identified included sources such as Defense Technical Information Center (DTIC), Naval Postgraduate School (NPS) Library, Institute of Electrical and Electronics Engineers (IEEE) Xplore, and the International Council On Systems Engineering (INCOSE).

Identify risks and uncertainty. Risk in the area of cost for the thesis development was low, since ample resources were allocated. Risk in the area of schedule was initially high, then dropped down to medium and then low as the scope of the thesis was reduced to mitigate the risk of a calendar-driven thesis. Risk in the area of technical performance was initially medium due to the uncertainty of available source information and data, and then was dropped down to low as the literature review resulted in useful information.

4. Evaluation Techniques

Select appropriate techniques. *Literature research and review* was the specific technique used to address the thesis research questions and evaluate the premise. No architecture products, mathematical models, software programs or simulations were required to address the research questions.

5. Obtain, Construct and/or Verify & Validate Models

Since formal models were not constructed as a product of this thesis, this step is not applicable.

6. Source Data Collection

The NPS Library was used to query the EBSCOhost, BOSUN, DTIC, and IEEE Xplore databases for professional journal articles, conference proceedings and DoD policies, directives, instructions, manuals and guides in search of information and data pertaining to the research questions.

The literature was initially scanned to determine whether the research questions had been previously addressed, or if the questions were otherwise easily answered by existing publications. This review turned up some very relevant reference documents, but no comprehensive, consolidated documentation that addressed the research questions in the context of the thesis premise.

The initial scan was followed by an in-depth literature review for pertinent information required to support the research questions.

7. Evaluation of Alternatives

The results of the research were evaluated and a determination was made on the validity of the premise, referencing supporting information and data.

8. Results and Recommendations

Findings associated with the research questions were discussed in the appropriate chapters and conclusions were drawn based on interpretation of the results in the context of the research questions. Recommendations were made for improvement of architecture integration processes. Conclusions were drawn regarding the validity of the thesis premise.

After the results and recommendations were coordinated with NPS, ASEO and AAIC, the final thesis was submitted to NPS for processing and distribution.

9. Iterate and Refine the Analysis

Feedback on the published thesis may generate more or expanded research questions, examples of which are given in the Future Work section of Chapter V. This thesis may be revisited for expansion or refocusing of the scope, in which case all or part of the methodology would be repeated, making the necessary modifications.

G. CHAPTER SUMMARY

This chapter provided an introduction to and an overview of this thesis, including the purpose, background, research questions, scope, benefits, and methodology.

THIS PAGE INTENTIONALLY LEFT BLANK

II. THE NEED FOR INTEGRATED ARCHITECTURES

A. INTRODUCTION

This chapter presents the results of the literature review on integrated architectures and their uses. Section B highlights the numerous references to architectures and their purposes throughout federal and DoD policy, directives, instructions, manuals and guides. Section C provides a brief overview of architecture framework and products, which are the means for documenting and relating architectural data. Section D describes features and characteristics of integrated architectures. Section E discusses the various uses for integrated architectures in supporting the DoD decision making processes. Section F summarizes the chapter.

B. POLICIES PERTAINING TO ARCHITECTURES

There are numerous references to the importance of using architectures throughout federal and DoD policies, some of which specifically call out the need for *integrated* architectures. There is additional policy that requires architectures to be used in analyses to support decision making.

Table 1 is an extract from the Department of Defense Architecture Framework (DoDAF) that shows federal policies pertaining to architectures. These policies call for the use of architectures to improve management of Information Technology (IT) resources; promote electronic government services and processes; facilitate cross-agency analysis and identification of duplicative investments, gaps, and opportunities for collaboration across Federal Agencies; and provide compliance criteria for assessing enterprise architecture management maturity.

Policy/Guidance	Description
Clinger-Cohen Act of 1996	Recognizes the need for Federal Agencies to improve the way they select and manage IT resources and states "information technology architecture, with respect to an executive agency, means an integrated framework for evolving or maintaining existing IT and acquiring new IT to achieve the agency's strategic goals and information resources management goals". Chief Information Officers are assigned the responsibility for "developing, maintaining, and facilitating the implementation of a sound and integrated IT architecture for the executive agency."
Office of Management and Budget Circular A-130	"Establishes policy for the management of Federal information resources"[15] and calls for the use of Enterprise Architectures to support capital planning and investment control processes. Includes implementation principles and guidelines for creating and maintaining Enterprise Architectures.
E-Government Act of 2002	Calls for the development of Enterprise Architecture to aid in enhancing the management and promotion of electronic government services and processes.
OMB Federal Enterprise Architecture Reference Models (FEA RM)	Facilitates cross-agency analysis and the identification of duplicative investments, gaps, and opportunities for collaboration within and across Federal Agencies.[16] Alignment with the reference models ensures that important elements of the FEA are described in a common and consistent way.[17] The DoD Enterprise Architecture Reference Models are aligned with the FEA RM.
OMB Enterprise Architecture Assessment Framework (EAAF)	Serves as the basis for enterprise architecture maturity assessments. Compliance with the EAAF ensures that enterprise architectures are advanced and appropriately developed to improve the performance of information resource management and IT investment decision making.
General Accounting Office Enterprise Architecture Management Maturity Framework (EAMMF)	"Outlines the steps toward achieving a stable and mature process for managing the development, maintenance, and implementation of enterprise architecture." Using the EAMMF allows managers to determine what steps are needed for improving architecture management.

15 Office of Management and Budget, http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html#2
16 E-Gov, http://www.whitehouse.gov/omb/egov/a-2-EAModelsNEW2.html
17 Consolidated Reference Model Version 2.0, http://www.whitehouse.gov/omb/egov/documents/FEA_CRM_v20_Final_June_2006.pdf

Table 1 Federal Policies Pertaining to Architectures (From: Table 3-1 in DoDAF, 2007)

Table 2 describes key processes that the DoDAF states are supported by architectures. The Joint Capabilities and Integration Development System (JCIDS), Planning, Programming, Budgeting, and Execution (PPBE), Defense Acquisition System, and Portfolio Management (PfM) are all DoD Decision Support Processes that rely on architecture data as a foundation upon which to base decisions. These processes are discussed later in the chapter.

Process	Description
Joint Capabilities Integration and Development System	"Requires a collaborative process that utilizes joint concepts and integrated architectures to identify prioritized capability gaps and integrated joint DOTMLPF and policy approaches (materiel and non-materiel) to resolve those gaps."[18] Incorporates the requirement for the net-ready key performance parameter (NR-KPP) in accordance with DoD Directive 4630.5[19], DoD Instruction 4630.8,[20] and Chairman Joint Chiefs of Staff (CJCS) Instruction (CJCSI) 6212.01D.[21]
Planning, Programming, Budgeting, and Execution	DoD policy has not formalized the use of architectures in the PPBE process but DoD Services, such as the Navy and Air Force, have noted that architectures provide a context for developing program priorities, formulating programmatic modifications, and making IT investment decisions.
Defense Acquisition System	Includes the requirement for an integrated architecture in developing integrated plans or roadmaps to conduct capability assessments, guide systems development, and define the associated investment plans as the basis for aligning resources.[22]
Portfolio Management	Calls for "the management of selected groupings of IT investments using strategic planning, architectures, and outcome-based performance measures to achieve a mission capability".[23]

18 CJCS Instruction 3170.01E, Joint Capabilities Integration and Development System (JCIDS), 11 May 2005 *(Author's note: this document has been superseded by CJCS Instruction 3170-01F, 1 May 2007)*
19 DoD Directive 4630.5, Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS), 5 May 2004
20 DoD Instruction 4630.8, Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems
(NSS), 30 June 2004
21 CJCS Instruction 6212.01D, Interoperability and Supportability of Information Technology and National Security Systems, 8 March 2006
22 DoD Instruction 5000.2, Operation of the Defense Acquisition System, 12 May 2003
23 DoD Directive 8115.01, Information Technology Portfolio Management, 10 October 2005

Table 2 Architectures in Support of DoD Decision Support Processes (From: Table 3-2 in DoDAF, 2007)

There are a number of additional policies, guides, instructions and manuals not mentioned in the DoDAF's summaries above, which also highlight the use of integrated architectures as an important source of data for supporting various analyses and life cycle processes. Table 3 presents additional policies and guidance that was reviewed in researching material for this chapter. The documents described in the tables range from directives and instructions to reference models and guides, and their bearing of each on architectures is summarized in the table. Tables 1, 2 and 3 lay the foundation for establishing the needs for architecture described in later sections.

Policy/Guidance	Description
DoDD 5000.1 (2003) The Defense Acquisition System	Joint concepts and integrated architectures shall be used to characterize interoperability among systems, units and forces (Para. E1.13). Systems concepts for products, services and technologies shall be consistent with joint integrated architectures (Para. E1.18).
DoDD 8100.1 (2002) Global Information Grid (GIG) Overarching Policy	"GIG assets shall be… compliant with the operational, system, and technical views (reference (f)) of the GIG architecture (reference (g))" (Para. 4.3). "The GIG shall be based on a common, or enterprise-level, communications and computing architecture" (Para. 4.4). "Reference (g) shall be the sound and integrated information technology architecture required by section 5125(b)(2) of the Clinger-Cohen Act of 1996 (reference (b))" (Para. 4.6). (b) Section 1401 et seq. of title 40, United States Code (f) C4ISR Architecture Framework, Version 2.0, 2 December 18, 1997 *(Author's note: this document has been superseded by the DoD Architecture Framework, Version 1.5, 23 April 2007)* (g) Global Information Grid Architecture, current version. This CD-ROM may be obtained from the DoD Office of the Chief Information Officer, Architecture & Interoperability Directorate (703) 607-0233.
CJCSM3170-01C (2007) Operation of the Joint Capabilities and Integration Development System (JCIDS)	The use of integrated architectures in the JCIDS process is referenced throughout this manual, which is based on the CJCS Instruction 3170-01F, JCIDS. It describes the JCIDS documents, their relationships with integrated architectures, and the iterative nature of JCIDS analysis and refinement of the integrated architectures. The JCIDS analyses assess capabilities of systems as a whole using integrated architectures of multiple interoperable systems rather than assessing capabilities in isolation (pp. 11-12, DAG, 2006).

Policy/Guidance	Description
CJCSI 6212.01D (2006) Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)	"Supporting integrated architecture products" required to assess information exchange and operationally effective use for a given capability is one of the four Net-Ready Key Performance Parameter (NR-KPP) elements. NR-KPPs consist of verifiable performance measures and metrics and are used to assess information needs, information timeliness, information assurance, and net-ready attributes required for both the technical exchange of information and the end-to-end operational effectiveness of that exchange (Para. 4c-d).
DoDD 4630.05 (2004) Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)	"IT and NSS interoperability and supportability needs shall be derived using Joint Operating Concepts, Joint Functional Concepts, and associated integrated architectures and shall be updated as necessary throughout the system's life" (Para. 4.3).
DoDI 4630.8 (2004) Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)	"Integrated architectures shall be used as the basis for assessment and analysis to characterize interoperability needs for a given capability" (Para. 6.1.3). "Integrated architectures are the common foundation for capability- focused, effects-based IT and NSS interoperability and supportability processes for ACAT-designated acquisitions, non-ACAT acquisitions or procurements, and fielded capabilities" (Para. 6.1.4).
NCOW RM (2005) Net-centric Operations and Warfare Reference Model	"Federal law and mandates require that the Chief Information Officers (CIOs) of all executive agencies develop, maintain, and facilitate the implementation of a sound and integrated IT (or enterprise) architecture for their respective agencies.[5]" (Para. 2.1, Introduction) [5] Public Law 104-106, Division E, the Clinger-Cohen Act ("The Information Technology Management Reform Act of 1996"); Title 40, United States Code, Section 1425, Agency Chief Information Officer, May 13, 2002; and Title 40, United States Code, Subtitle III, Information Technology Management, January 28, 2005.

Policy/Guidance	Description
DoDD 8000.01 (2002) Management of DoD Information Resources and Information Technology	"An integrated DoD architecture with operational, system, and technical views shall be developed, maintained, and applied to determine interoperability and capability requirements, promote standards, accommodate the accessibility and usability requirements of reference (k), and implement security requirements across the DoD enterprise to provide the basis for efficient and effective acquisition and operation of IT capabilities" (Para. 4.4.3). (k) Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. 794d).
DoDD 8115.1 (2005) Information Technology Portfolio Management	"IT investments shall be managed as portfolios.... Each portfolio shall be managed using the GIG architecture (reference (e)), plans, risk management techniques, capability goals and objectives, and performance measures" (Para. 4.1.). "The Assistant Secretary of Defense for Networks and Information Integration/Department of Defense Chief Information Officer (ASD(NII)/DoD CIO) shall… ensure that all Mission Area portfolio recommendations are based on architectures that comply with reference (e) and DoD Directive 8500.1 (reference (j))" (Para. 5.1) (e) DoD Directive 8100.1, "Global Information Grid (GIG) Overarching Policy," September 19, 2002 (j) DoD Directive 8500.1, "Information Assurance (IA)," October 24, 2002

Policy/Guidance	Description
Transformation Planning Guidance (2003)	“Leveraging information technology and innovative concepts to develop an interoperable, joint C4ISR architecture and capability that includes a tailorable joint operational picture will guarantee our combat leaders decision superiority and enable our forces to maneuver effectively to gain positional advantage, avoid battlefield obstacles and successfully attack the adversary even in the face of numerically superior forces.” (p. 11) “Integrated architectures describe in greater detail the relationship between the tasks and activities that generate effects on enemy forces and supporting operations. They identify where operations intersect and overlap and they provide details on interoperability requirements. The architectures will include not just material solutions but also doctrine, organization, and training needs. Using these architectures, the JROC [Joint Requirements Oversight Council] will be responsible for prioritization of capabilities based on their contribution to realization of the JOCs [Joint Operating Concepts].” (p. 16) “As the Department transforms to a joint concept-centric approach to operational planning and capabilities development, we need integrated architectures that define the specific parameters of the requisite joint capabilities.” (p. 20)
Introduction to Defense Acquisition Management (2005)	“Achieving full spectrum dominance also means building an integrated, complex set of systems, especially a command, control, communications, computers, intelligence, surveillance and reconnaissance architecture.” (p. 11) A system architecture (defined set of subsystems making up the system), and an operational architecture (description of how this system interacts with other systems, to include passing of data), are called out as requirements for entrance into the System Development and Demonstration (SDD) Phase of the acquisition lifecycle (p. 53). Integrated Architectures support joint force commanders in integrating “a set of related military tasks to attain capabilities required across the range of military operations” (p. 43).

Policy/Guidance	Description
Defense Acquisition Guidebook (2006)	“A technical framework, including essential architecture products, is necessary for a program manager to initiate the systems engineering process to allow interoperability with legacy, current, and future systems.” (Section 4.5.7.1) “The Global Information Grid (GIG) is the organizing and transforming construct for managing information technology (IT) throughout the Department. GIG policy, governance procedures, and supporting architectures are the basis for developing and evolving IT capabilities, IT capital planning and funding strategies, and management of legacy (existing) IT services and systems in the DoD.” (Section 7.2.1) “As the Secretary of Defense’s principal staff assistant for IT and information resources management, the CIO develops, maintains, and uses the Department’s enterprise IT architecture--the Global Information Grid (GIG) Architecture and the Net-Centric Operations and Warfare (NCOW) Reference Model to guide and oversee the evolution of the Department’s IT-related investments to meet operational needs.” (Section 7.2.1.3) Architecture documentation is “required in the Joint Capabilities Integration and Development System documents: Initial Capabilities Document, Capability Development Document, and Capability Production Document.” (Section 7.3.6)
Test & Evaluation Management Guide (2005)	Architectures of systems are represented in the context of their support to acquisition life cycle phases and milestones, and with respect to test & evaluation (Figure 1-1, Figure 17.3, and Figure 20-4).

Policy/Guidance	Description
DoD Risk Management Guide (2006)	Although the Risk Management Guide does not explicitly call out architectures specifically, it strongly suggests involvement of the architecture and its developers in risk analysis through program aspects and parameters captured by architectures. "Risk can be associated with all aspects of a program, e.g., operational needs, attributes, constraints, performance parameters including Key Performance Parameters (KPPs), threats, technology, design processes, or WBS [Work Breakdown Structure] elements. Consequently it is important to recognize that risk identification is the responsibility of every member of the IPT [Integrated Product Team], not just the PM or systems engineer." (Section 3.2)
Guide to SoSE (2006) Guide to Systems of Systems (SoS) Engineering: Considerations for Systems Engineering	This guide puts architecture into the context of a broader system of systems engineering (SoSE) process used for: • identifying the necessary SoS capabilities; • assessing availability and relevance of assets within existing systems portfolios; • developing the necessary "architecture" that becomes the integrating framework for the conceived system of systems; • allocating capabilities to a set of interdependent existing, under-development, or yet to be developed systems; and • coordinating and integrating all the necessary development, production, sustainment, and other activities throughout the life cycle of a SoS. (Section 2.2.2)
SEP Preparation Guide (2006) Systems Engineering Plan Preparation Guide v1.02	This guide recommends that the Systems Engineering Plan for a program includes "an overview of the approach and methods planned for use in arriving at a balanced set of requirements and a balanced functional and design architecture to satisfy those requirements." (Section 3.4.3)

Table 3 References to Integrated Architectures throughout Other Policies, Guides, Instructions, and Manuals

C. ARCHITECTURE FRAMEWORK

Recall the definitions of architecture and integrated architecture from Chapter I:

Architecture – “the structure of components, their relationships, and the principles and guidelines governing their design and evolution over time.” (p. xiv, Volume II, DoDAF, 2007)

Integrated architecture – “an architecture consisting of multiple views or perspectives (operational view, systems view, and technical standards view) that facilitates integration and promotes interoperability across capabilities and among related integrated architectures.” (p. GL-9, CJCSI 3170.01F, 2007)

The large amount of information associated with these architectures requires a framework in which it can be stored, related, and integrated. Governments and industries use *enterprise architecture frameworks*, which are “set[s] of operational guideline[s] and rules to follow to manage and align an organization’s operations and projects with their overall strategy” (Griffin, 2005). DoD Instruction 5000.2 mandates that each integrated architecture have operational, systems, and technical views as defined in the current Architectural Framework guidance (Section 3.2.1.2, DoDI 5000.2, 2003). The DoD Architecture Framework (DoDAF) Version 1.5 published in April 2007 is the current Architectural Framework guidance, with version 2.0 under development (Volume I, Section 2.1, DoDAF, 2007). Version 1.5 has an additional view not specifically called out in DoD Instruction 5000.2 – the All View (AV), which is an overview and summary document of the architecture.

The DoDAF 1.5 is a compendium of three volumes and one journal containing nearly nine hundred pages detailing architectural views and data, use and reuse of architecture data in decision-making processes, policy references to architectures, development of net-centric architectures, and various approaches and best practices for developing architectures and architecture products. The DoDAF is a foundation for “developing, representing, and understanding architectures based on a common denominator across DoD, Joint, and

The DoDAF states that an architecture description is "composed of *architecture products* that are interrelated within each view and are interrelated across views." A data model called the Core Architecture Data Model (CADM) (CADM, 2007) underlies the products and provides a standard set of data entities and relationships for the architecture data represented in the products. Integrated architecture products perform the following functions, as described in (Section 7.0.2, DAG, 2006):

- Describe existing and desired capabilities
- Provide a basis for interoperability and supportability reviews and certifications
- Provide a component of the Net-Ready Key Performance Parameter
- Provide required components of the Capability Development Document (CDD) and Capability Production Document (CPD), two of the required JCIDS documents
- Develop and describe Key Interface Profiles (KIPs). DAG Section 7.3.4.2 defines a KIP as a "set of documentation produced as a result of interface analysis which: designates an interface as key; analyzes it to understand its architectural, interoperability, test and configuration management characteristics; and documents those characteristics in conjunction with solution sets for issues identified during the analysis."
- Document consistency with the GIG architecture and policies.

In terms of what they look like, architecture products are graphical, textual, and tabular representations of the data that are developed in the course of:

- Gathering architecture data
- Identifying their composition into related architecture components or composites
- Modeling the relationships among those composites (Volume II, Section 1.2, DoDAF, 2007).

In other words, architecture products are used as vehicles for gathering and relating data that describes the architecture, and for modeling these relationships. The fact that the DoDAF describes architecture products in the context of modeling implies that the architecture products are not intended to be static, but dynamically updatable based on modeling results.

In an integrated architecture framework, all of the Operational Views (OVs), Systems and Services Views (SVs), and Technical Standards Views (TVs) are connected and consistent with one another. The All View (AV) contains high-level summary information about the architecture and includes references to the OVs, SVs, and TVs that make up the architecture. Table 4 provides the DoDAF descriptions for each type of view (Volume I, Section 1.4, DoDAF, 2007). The Appendix provides a short description of each view in version 1.5 of the DoDAF.

View	Description
All View (AV)	There are some overarching aspects of an architecture that relate to all three views. These overarching aspects are captured in the AV products. The AV products provide information pertinent to the entire architecture but do not represent a distinct view of the architecture. AV products set the scope and context of the architecture. The scope includes the subject area and time frame for the architecture. The setting in which the architecture exists comprises the interrelated conditions that compose the context for the architecture. These conditions include doctrine; tactics, techniques, and procedures; relevant goals and vision statements; concepts of operations (CONOPS); scenarios; and environmental conditions.
Operational View (OV)	The OV captures the operational nodes, the tasks or activities performed, and the information that must be exchanged to accomplish DoD missions. It conveys the types of information exchanged, the frequency of exchange, which tasks and activities are supported by the information exchanges, and the nature of information exchanges.
Systems and Services View (SV)	The SV captures system, service, and interconnection functionality providing for, or supporting, operational activities. DoD processes include warfighting, business, intelligence, and infrastructure functions. The SV system functions and services resources and components may be linked to the architecture artifacts in the OV. These system functions and service resources support the operational activities and facilitate the exchange of information among operational nodes.
Technical Standards View (TV)	The TV is the minimal set of rules governing the arrangement, interaction, and interdependence of system parts or elements. Its purpose is to ensure that a system satisfies a specified set of operational requirements. The TV provides the technical systems implementation guidelines upon which engineering specifications are based, common building blocks are established, and product lines are developed. It includes a collection of the technical standards, implementation conventions, standards options, rules, and criteria that can be organized into profile(s) that govern systems and system or service elements for a given architecture.

Table 4 Architecture View Descriptions

These views and their interrelationships “provide the basis for deriving measures such as interoperability or performance, and for measuring the impact of the values of these metrics on operational mission and task effectiveness” (Volume I, Section 1.4.1, DoDAF, 2007). The architect must be continuously aware of the interrelationships in order to produce an architecture that is consistent across all four views, and to provide clear traceability from one view to another (Volume II, Section 2.4, DoDAF, 2007). The views may be developed in an iterative manner, at different levels of abstraction or detail depending on the decision point supported and/or the intended audience. “Iterative development crosses all views. OVs can drive SV and TV changes; SVs can drive OV and TV changes, and so forth” (Volume II, Section 2.3.3, DoDAF, 2007). Figure 3 illustrates the linkages among the types of views.

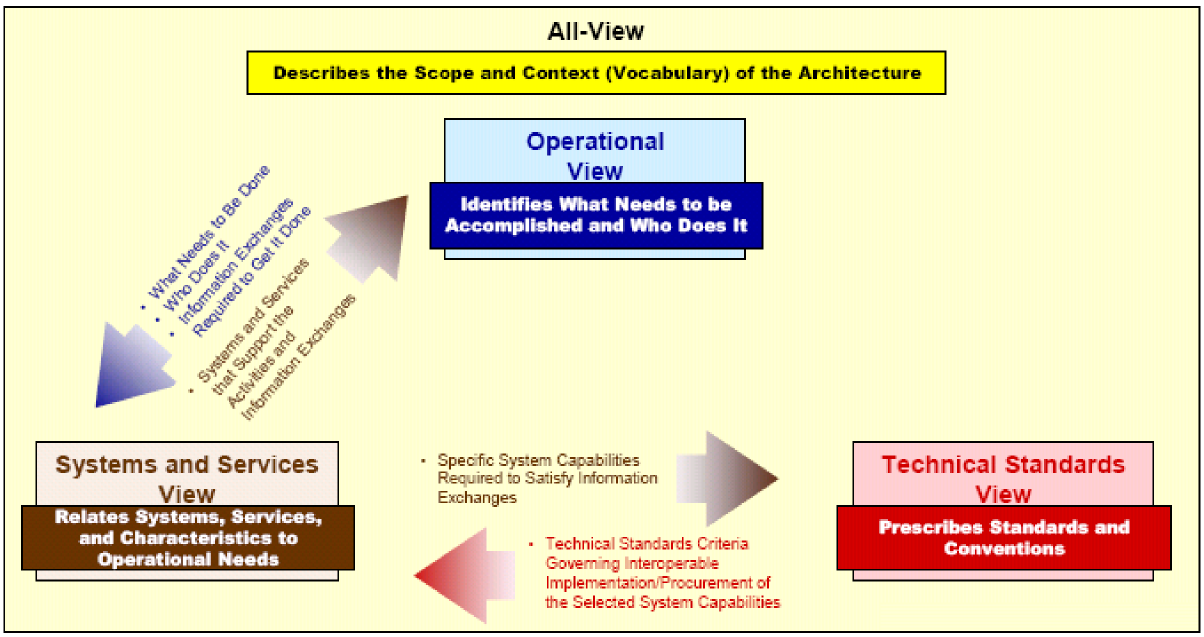


Figure 3 Linkages Among the Architecture Views (From: Figure 1-3 in Volume I, DoDAF, 2007)

For more information on the DoDAF and a comparison to other architecture frameworks, see (DoDAF, 2007) and (Griffin, 2005), respectively.

D. FEATURES OF INTEGRATED ARCHITECTURES

The DoDAF version 1.5 (Volume I, Section 1.2.2) defines the following characteristics of integrated architectures:

- Contains a mapping or standardization of terms, definitions, and relationships across the architecture
- Architectural objects common *to more than one view* are identical or linked via underlying data relationships

- All objects that have *relationships across views* are linked via underlying data relationships.

Since integrated architectures have common points of reference within the architecture description linking the views, they enable the following activities (Volume I, Section 1.2.2, DoDAF, 2007):

- Analyses of a broader scope than what is needed or possible through a single architectural view
- Clarification of roles, boundaries, and interfaces between components of large systems of systems
- Enterprise-level systems integration.

These logical linkages among the architecture data elements ensure that "the single architecture so described can actually be built and operated. In particular, these linkages ensure that the architecture remains mutually consistent. The linkages provide traceability from view to view, from product to product within a view, and across views that ensures:

- Integration of systems within a family of systems (FoS) or SoS
- Alignment of IT functionality to mission and operational needs
- Relationships between current and future systems to current and future standards
- Integration of services within a service family" (Volume II, Section 7.1, DoDAF, 2007).

The DoDAF has also defined a set of guidelines for use in developing architectures. These guidelines are critical to the development and integration of architectures that have a practical use by program, DoD Component, mission and enterprise-level decision makers. Table 5 summarizes these guidelines. For the full description, see (Volume I, Section 2.1, DoDAF, 2007).

Para.	Guideline	Description
2.1.1	Have a Purpose in Mind	• A specific and commonly understood purpose increases efficiency of the effort and the utility of the resulting description • The purpose determines the scope, which drives the specification of characteristics, time frames, data requirements, and level of detail • The purpose should align with the priorities of the community and contribute to the success of mission goals and objectives
2.1.2	Be Simple and Straightforward	• Developing overly complex architectures is costly • Focusing the architecting effort is essential to obtaining an acceptable return on investment • Care should be given in determining the level of detail appropriate for achieving the desired objectives of the architecture effort
2.1.3	Be Understandable Among Architecture Users	• Being understandable enhances the applicability of the information among architecture users • Architectures should guide the human thinking process in discovering, analyzing, and resolving issues quickly • Architectures should provide a clear representation of the information by using common terms and definitions and avoiding extraneous information
2.1.4	Be Interoperable Across the DoD	• Architectures should be expressible using a standard vocabulary with unambiguous semantics and a well defined data structure for comparison across independently developed models • Architecture descriptions must clearly describe external interfaces with Joint, multinational, and commercial components, and consistently with the method used to describe internal relationships • Architecture descriptions should be readily available across the Enterprise for decision process analyses, reuse in other architecture efforts, and mission support
2.1.5	Be Agile	• Architectures should be modular, reusable, and decomposable to achieve agility • Architecture descriptions should consist of related pieces that can be recombined with a minimal amount of tailoring to enable use for multiple purposes • An agile architecture provides the means for functioning in a dynamic environment

Table 5 DoDAF Guidelines for Architectures

These guidelines for architecture development and features of integrated architectures are further discussed in Chapter IV in the context of their applicability to the objectives of the Army Architecture Integration Process (AAIP), and their usability as criteria for measuring architecture quality and integrity.

E. USES FOR INTEGRATED ARCHITECTURES

As can be seen from the summary of policies and guidance earlier in this chapter, architectures are used to support a variety of DoD processes. The most recurrent theme encountered throughout the literature is the use of architectures to support decision making. This section presents the uses of architecture surveyed in the literature in this most prevalent context of decision support, from Joint requirements oversight at the enterprise level to system design at the component and program levels.

Architectures are heavily relied upon for informing the DoD decision support processes (i.e., JCIDS, Planning, Programming, Budgeting, and Execution (PPBE), Defense Acquisition System (DAS), and Portfolio Management (PfM)). An excerpt from (Section 7.2.9, DAG, 2006), Table 6 is provided as an exemplar description of how the DoD CIO uses the DoD's enterprise architecture, the GIG Architecture, in all three of these decision processes.

Some of the general uses of architectures that have already been highlighted include:

- Improvement of management of Information Technology (IT) resources
- Promotion of electronic government services and processes
- Facilitation of cross-agency analysis and identification of duplicative investments, gaps, and opportunities for collaboration across Federal Agencies
- Provision of compliance criteria for assessing enterprise architecture management maturity

- Support to key DoD decision support processes (i.e., JCIDS, PPBE, DAS, and IT PfM)

Drawing on the uses summarized above, the DoDAF has created an organization scheme for the types of uses of architecture data for supporting different types of decisions, using the following five categories: Enterprise and Portfolio Management, Capability and Interoperability Readiness, Acquisition Program Management and System Development, Modeling and Simulation (M&S), and Operational Planning. Although not comprehensive, the paragraphs below elaborate and expand on many of the uses presented in Tables 1, 2 and 3 following the five categories provided by the DoDAF.

1. Enterprise and Portfolio Management

The DoDAF executive summary states that "experience has demonstrated that the management of large organizations employing sophisticated systems and technologies in pursuit of joint missions demands a structured, repeatable method for evaluating investments and investment alternatives, implementing organizational change, creating new systems, and deploying new technologies." *Information Technology (IT) investments* are resources required to support IT or IT-related initiatives, which include research, development, test, and evaluation appropriations; procurement appropriations; military personnel appropriations; operations and maintenance appropriations; and Defense Working Capital Fund (Para. E2.1.4, DoDD 8115.1, 2005). These IT investments undergo a process called *Portfolio Management (PfM)*, which is the "management of selected groupings of IT investments using strategic planning, architectures, and outcome-based performance measures to achieve a mission capability" (Para. E2.1.8, DoDD 8115.1, 2005).

The DoD CIO uses the GIG architecture throughout the processes included in operating the Joint Capabilities Integration and Development System to: • Advise the Joint Requirements Oversight Council. • Provide the basis for the development and refinement of joint integrated architectures by the Joint Staff and other DoD Components in support of the Joint Capabilities Integration and Development System. • Develop assessments and provide recommendations to the JROC; the GIG Architecture, including its concepts, products, data, conclusions, and implications provides a key source for these assessments. The DoD CIO uses the GIG architecture throughout the Planning, Programming, Budgeting, and Execution process to: • Review and provide recommendations for development of the Strategic Planning Guidance and the Joint Programming Guidance. • Provide recommendations to the Senior Level Review Group relating to Information Technology, National Security Systems, interoperability, and information assurance. • Review and evaluate Program Change Proposals and Budget Change Proposals relating to Information Technology, National Security Systems, interoperability, and information assurance. • Provide recommendations for Program Objective Memorandum planning and programming advice. Finally, the DoD CIO uses the GIG Architecture throughout the Defense Acquisition Process to: • Provide the basis for clear and comprehensive guidance in Information Technology Acquisition Decision Memoranda. • Form and support his decisions and recommendations as a member of the Defense Acquisition Board, the lead for the Information Technology Acquisition Board, and the Milestone Decision Authority for Acquisition Category IA programs. • Identify and specify Information Technology and National Security Systems implications associated with systems acquisition. • Assess interoperability and supportability during the Overarching Integrated Product Team process. • Review Information Support Plans and evaluate the interoperability, interoperability key performance parameters, and information assurance aspects of those plans.

Table 6 Use of the GIG Architecture in Support of Major Decision Processes (From: Section 7.2.9, DAG, 2006).

The purpose of PfM is to direct IT investments according to DoD's vision, mission, and goals; deliver efficient and effective capabilities to the warfighter; and maximize return on investment to DoD (Para. 4.1, DoDD 8115.1, 2005). There are three levels of portfolios: Enterprise (the top-level portfolio), Mission Area (the portfolio level under Enterprise), and Component (the portfolio level under Mission Area). "Enterprise" refers to the DoD and all of its organizational entities (Para. E2.1.2, DoDD 8115.1, 2005). A Mission Area is "a defined area of responsibility with functions and processes that contribute to mission accomplishment" (Para. E2.1.7, DoDD 8115.1, 2005). Mission Areas and Components may be further divided into sub-portfolios (a.k.a. domains) or capability areas that "represent common collections of related, or highly dependent, information capabilities and services" (Para. 4.2, DoDD 8115.1, 2005). Figure 4 is a graphical depiction of the portfolio levels. Portfolios are used as a management tool in each of the DoD's decision support systems listed in Table 2 and pictured at the top of Figure 5.

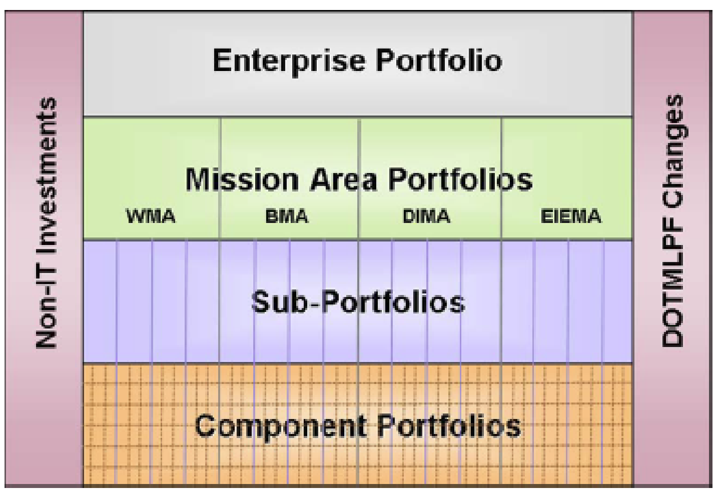


Figure 4 IT Portfolios (From: Figure 3 in DoDI 8115.02, 2006)

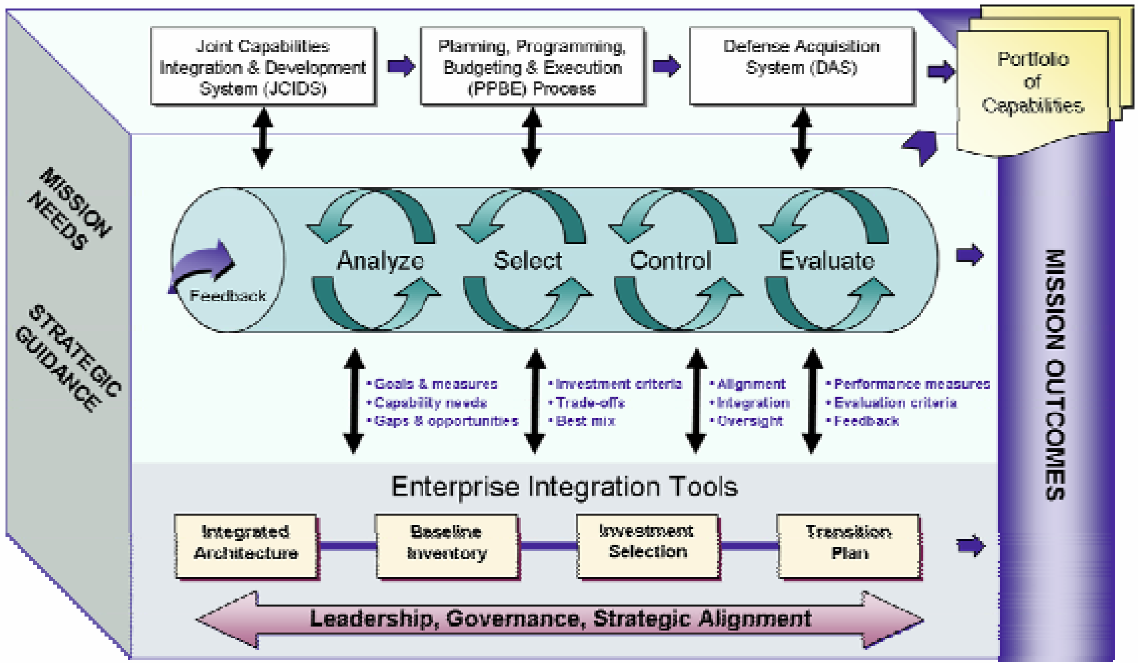


Figure 5 IT Portfolio Management Decision Support Interactions (From: Figure 1 in DoDI 8115.02, 2006)

As noted in the earlier definition of PfM, and shown in Figure 5, architectures are used to support the evaluation of IT investments. Architectures convey necessary information to decision makers at every portfolio level, as is described below (Volume I, Section 3.1, DoDAF, 2007).

At the Enterprise Portfolio level, architectures are used to make decisions to improve (1) human resource utilization, (2) deployment of assets, (3) warfighter investments, and (4) identification of the enterprise boundary (interfaces) and assignment of functional responsibility.

At the Mission Area Portfolio level, architectures are used to manage capabilities within and across mission areas and improve investment decisions. Architectures at this level are also used to provide roadmaps and descriptions of future or desired end states.

At the Component/Program Portfolio level, architectures are used to "identify capability requirements and operational resource needs that meet business or warfighting objectives."

Component and Program architectures may be integrated and aggregated to support decision making at the mission level, and mission level architectures integrated and aggregated to support decision making at the enterprise level. "Rolling up component and program-level architectures to the enterprise ensures complete, actionable information for more reliable decisions" (Volume I, Section 3.1, DoDAF, 2007), and provides decision makers with traceability to hard data.

A specific example of how architectures are used to support PfM is its enabling of the identification of "opportunities to satisfy multiple operational requirements with a single, leveraged capability" (Volume I, Section 3.1, DoDAF, 2007). One approach for doing such an analysis may be to use the rolled up information provided in PfM to look at the various capabilities of component architectures, and determine whether one of these capabilities can be provided to all the component architectures to efficiently satisfy the operational requirements of each architecture. The ability to make such an identification would save valuable resources that would otherwise be spent on needlessly developing and/or maintaining separate and possibly non-interoperable capabilities. Another benefit of such an analysis may be the identification of an existing capability that can be leveraged in another architecture to satisfy an as-yet unaddressed operational requirement.

2. Capability and Interoperability Readiness

This function pertains to the assessment of net-readiness by identifying gaps in interoperable capabilities (Volume I, Section 3.1, DoDAF, 2007). Net-readiness refers to the "ability of systems to enable warfighters to exercise control over enterprise information and services" (p. 7, Hutchens, 2007). A Key Performance Parameter (KPP) known as the Net-Ready KPP (NR-KPP) has been developed specifically to assess information needs, information timeliness, information assurance, and net-ready attributes that are required for the technical exchange of information, as well as the end-to-end operational effectiveness of that exchange. The NR-KPP incorporates net-centric concepts for achieving IT and National Security Systems (NSS) interoperability and supportability (Section 7.3.4, DAG, 2006).

The NR-KPP consists of measures of performance and metrics for evaluating the "timely, accurate, and complete exchange and use of information to satisfy information needs for a given capability" (Section 7.3.4, DAG, 2006). *Supporting integrated architecture products* is one of four NR-KPP elements, as noted from CJCS Instruction 6212.01D in Table 3 earlier in this chapter. (The other elements are: *Compliance with the Net-Centric Operations and Warfare Reference Model*, *Compliance with applicable Global Information Grid Key Interface Profiles*, and *Compliance with DoD Information Assurance requirements.*) Program Managers are required to comply with this element of the NR-KPP by demonstrating conformance with DoDAF specifications and that all required views have been produced per the procedures detailed in CJCS Instruction 3170.01 and CJCS Instruction 6212.01. (Section 7.3.4.5, DAG, 2006). All four elements of the NR-KPP inform the Defense Acquisition Process by assisting Program Managers, the test community, and Milestone Decision Authorities in conducting assessments and evaluations of IT and NSS interoperability. The NR-KPP, which is documented in both the Capability Development Document (CDD) and Capability Production Document (CPD), is used for analysis, identification, and description of IT and NSS interoperability needs specified in the Information Support Plan, and in the test strategies in the Test and Evaluation Master Plan (Section 7.3.4, DAG, 2006).

3. Acquisition Program Management and Systems Development

Architecture data supports program management and systems development by representing system concepts, design, and implementation as they mature over time, which enable and support operational requirements. The architecture data also includes traceability of system design to operational requirements (Volume I, Section 3.1, DoDAF, 2007). This section of the DoDAF further states that "this process simplifies and integrates operational and system analysis, and improves both materiel and non-materiel solution analysis."

The JCIDS (CJCS Instruction 3170-01F and CJCS Manual 3170-01C) extensively describes the use of integrated architectures throughout the defense acquisition process. The JCIDS implements a capabilities-based methodology that "leverages the expertise of all government agencies to identify improvements to existing capabilities and to develop new warfighting capabilities." (Enclosure A, Para. 2, CJCSI 3170.01F, 2007). A Capabilities-Based Assessment (CBA) is conducted to identify capability needs, capability gaps, capability excesses, and approaches to provide needed capabilities within a specified functional or operational area (Enclosure A, Para. 1, CJCSI 3170.01C, 2007). According to the CJCSI 3170.01F Glossary, a *capability need* is defined as a capability that is required to be able to perform a task within specified conditions to a required level of performance; and a *capability gap* is what results from the "inability to achieve a desired effect under specified standards and conditions through combinations of means and ways to perform a set of tasks. The gap may be the result of no existing capability, lack of proficiency or sufficiency in existing capability, or the need to recapitalize an existing capability."

JCIDS advises that the CBA "include information and analysis that will support development of integrated architectures that are used to fully define solutions to capability gaps" and "use existing architectures as means of assessing current and programmed approaches to the military problems being assessed." CBA results, and by extension any existing architectures on which they are based, are also used to support analysis of alternatives (AoA). Furthermore, joint experimentation (CJCSI 3010.02 Series, 2007) and technology development are linked to existing architectures on which CBA results are based. "The results of experimentation may be used as input to the CBA; or, the results of the CBA may direct new experimentation efforts or identify areas where additional technology development is required to deliver the required capability"

(Enclosure A, Para. 1g, CJCSI 3170.01C, 2007). Therefore, by extension, experimentation and technology development both influence and are influenced by the architectures upon which the CBA is based.

Figure 6 illustrates the centrality of integrated architectures to the CBA process. CBA analysis is depicted by the shaded areas of functional area analysis (FAA), functional needs analysis (FNA), and functional solution analysis (FSA). The results of the CBA are the basis for the JCIDS documents, which, in turn, guide / are guided by the evolution of the integrated architecture throughout the remaining JCIDS process (Figure 7). In particular, “key components of the CDD and CPD are the integrated architecture products that ensure the Department of Defense understands the linkages between capabilities and systems and can make appropriate acquisition decisions; and the performance attributes, including KPPs and key system attributes (KSAs), that define the most critical elements of performance for the systems under development” (Enclosure A, Para. 3a, CJCS Instruction 3170-01F, 2007).

The CDD specifies the planned technical performance criteria of the system, whereas the CPD describes the actual performance of the system that will go into production. The main difference between a CPD and a CDD is that the CPD is informed by the lessons learned during development (Para. 4d, CJCSI 3170.01F, 2007). Integrated architectures guide the development of both the CDD and the CPD (Enclosure F/G, Para. 1a, CJCSI 3170.01C, 2007).

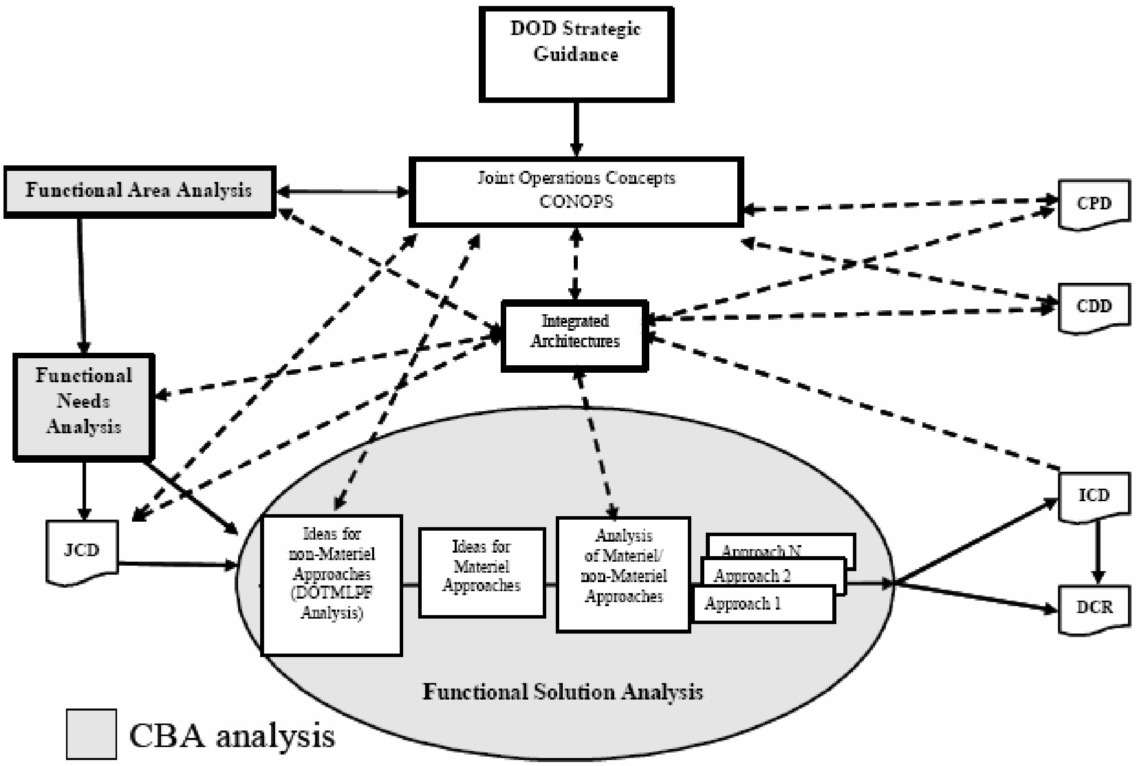


Figure 6 The Centrality of Integrated Architectures to the Capabilities-Based Assessment (From: Figure A-2 from CJCSM 3170.01C, 2007)

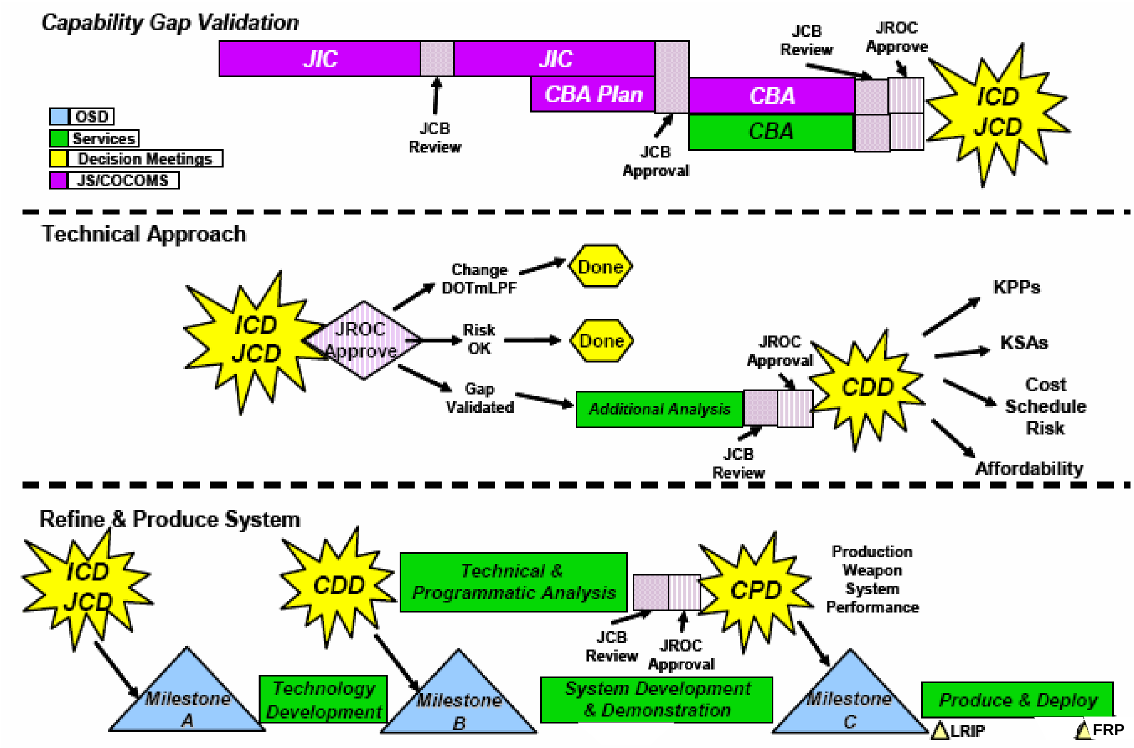


Figure 7 JCIDS Process and Acquisition Decisions (From: Figure A-2 in CJCSI 3170.01F, 2007)

Another key use of architecture data in acquisition program management and systems development is to prepare the Information Support Plan (ISP). The Defense Acquisition Guidebook (Section 7.3.6) states that "the ISP will use the architecture documentation from the Joint Capabilities Integration and Development System documentation and focus on analysis." The ISP identifies IT and information needs, dependencies, and interfaces for acquisition and non-acquisition programs, particularly dealing with net-readiness, interoperability, information supportability, and information sufficiency (DODI 4630.8, 2004). This document is used to identify and resolve implementation issues (Para. E4.1.2, DODI 4630.8, 2004), and implements a process of discovery "requiring an analysis of the program's integrated architecture" (Para. E4.1.3, DODI 4630.8, 2004). This analysis of the architecture is conducted to identify interoperability and supportability issues, and to assess compliance with DoD information policy and goals.

The ISP addresses the following fundamental questions for each piece of information needed to support the program's operational and/or functional capability(ies) (Paras. E4.1.3.1-E4.1.3.7, DODI 4630.8, 2004):

- What information is needed by the program to successfully execute the capability(ies)?
- How accurate must the information be?
- What quantity of information is needed (or in the case of information sources, what should be provided)?
- How shall the information be obtained (or access provided)?
- How quickly must the information be received to be useful?
- Does the program implementation comply with net-centric concepts?
- Does the program or capability comply with DoD IT and NSS policies?

In acquisition programs, an initial ISP is required at Milestone B, and an updated ISP is required at Milestone C (Table G-1, CJCSM 3170.01C, 2007).

4. Modeling & Simulation

The Department of Defense is transforming to network-centric operations and the use of "individually-complex systems linked together in complex systems-of-systems." Despite the dramatic increase in complexity in an SoS construct, a high expectation remains for seamless interoperability while maintaining effective performance by each individual system. Modeling & Simulation is a tool that is used throughout the acquisition lifecycle to "rapidly field improved capabilities with sufficient confidence that the fielded capabilities will perform effectively in the system-of-systems joint mission environment" (Section 4.5.7, DAG, 2006).

A *model*, in the context of science and engineering, is a representation of a system, and *simulation* is the process of manipulating a model "to explore the effects of alternative system characteristics on system performance without actually producing and testing each candidate system" (Section 7.2, Blanchard & Fabrycky, 2006). Most models fall into one of the following four classifications:

physical, analogue, schematic, or mathematical. Physical models are "geometric equivalents" that are larger, smaller, or equal in scale to the system it is modeling, such as a model airplane. An analogue model is similar in relation to the system it is modeling, but is represented differently, such as electric circuits representing mechanical systems, or electronic components in computers representing the dynamic loading of structures. A schematic model represents states or events as a chart or a diagram, such as the execution of a football play on a blackboard, or an organization chart showing relationships between various members within that organization. Finally, a mathematical model uses the language of mathematics to describe, predict, or control system behavior. For example, physical phenomena may be described by mathematical models incorporating Ohm's law and Newton's laws of motion, and profit levels associated with various production quantities of multiple types of products may be described by a linear program. Mathematical modeling is distinguished from the modeling of physical sciences in that they often include probabilistic elements to capture the random behavior of social, economic and other uncertain factors. Furthermore, unlike physical science models, they include two classes of variables: uncontrollable variables whose values cannot be controlled directly; and controllable variables for which optimal values can be selected by the decision maker in order to optimize some measure of effectiveness (Section 7.2.1, Blanchard & Fabrycki, 2006).

The use of Modeling & Simulation (M&S) that is highlighted in the DoDAF is its use for modeling and simulating "the implementation of mission threads and scenarios, thus providing an environment for thorough testing of identified use cases" (Volume I, Section 3.1, DoDAF, 2007). The Defense Acquisition Guidebook provides a more extensive description of the applications of M&S (Section 4.5.7, DAG, 2006) in general, and in each of the life cycle phases (Concept Refinement, Technology Development, System Development and Demonstration, Production, and Operations & Support). "M&S plays an important role in all aspects of the acquisition process. This is especially true in designing and developing a capability that is part of a FoS or SoS. Today's systems and associated interactions are complex. M&S can assist the process by controlling the desired variables to provide a repeatable audit trail that can assist in the acquisition decision processes" (Section 4.5.7.5, DAG, 2006). Following is a description of the contributions of M&S to each life cycle phase. Architecture data informs all of the M&S-based analyses outlined below, since it is used as source data for modeling & simulation (Volume I, Section 3.1, DoDAF, 2007).

M&S can be used during Concept Refinement to (Section 4.5.7.1, DAG, 2006):

- help define a technical framework, including essential architecture products, to be part of the Capability Development Document.
- support a "collaborative process, to exchange data, consider alternatives (such as operational concepts, conceptual designs, cost, and technology strategies), and view potential resulting capabilities."
- "allow a program manager to conduct rapid virtual prototyping with all stakeholders playing a role in the system as part of a family-of-systems or systems-of systems."
- provide tools that can "be leveraged throughout successive phases of the acquisition cycle. Ideally, the same architecture, scenarios, data, and M&S exercised in the collaborative environment during concept refinement will be reused in support of the analysis during the Technology Development."

M&S can be used during Technology Development to (Section 4.5.7.2, DAG, 2006):

- "help reduce technology risk and determine an appropriate set of technologies to integrate into a full system."
- examine new technologies using architecture, scenario, data, hardware in the loop (HWIL), software in the loop (SWIL), and infrastructure data in a collaborative environment.
- determine how to interface "new technologies with legacy systems and determine the likelihood of their successful transition to support a needed capability."
- examine reliability, maintainability, transportability, provisioning (spares, support equipment, manpower), cost implications, and human-machine interface design considerations.

- conduct stress analysis, structural dynamics, mass properties, structural design materials, fatigue, loads, shock isolation, and acoustics.
- inform cost models and manpower estimates that determine projected life-cycle costs of the system.
- coordinate and integrate operational tests throughout the development process and incorporate them into developmental tests.
- develop, evaluate and redesign, and reevaluate virtual prototypes as appropriate using the "model-test-fix-mode" process.
- inform system performance specifications, the Test & Evaluation Master Plan (TEMP), an updated Systems Engineering Plan (SEP), validated systems support, Lifecycle cost estimates, and manpower requirements.

M&S can be used during Systems Development and Demonstration to (Section 4.5.7.3, DAG, 2006):

- identify required systems interface requirements (in conjunction with HWIL, real world Command, Control, Communications, Computers, Intelligence, Surveillance, Reconnaissance (C4ISR) systems, and other simulated systems).
- “support the testing process to evaluate the performance and maturity of the technology under development” (in conjunction with validated test data).
- “help focus T&E of hardware prototypes to maximize the highest pay off of the T&E investments.”
- assess a “system in scenarios and areas of the mission space or performance envelope where testing cannot be performed, is not cost effective, or additional data are required.”
- examine interactions among assets within a FoS or SoS via simulation when it is cost prohibitive and unrealistic to bring together all these assets to conduct live tests and evaluations of the systems' interactions.
- demonstrate a system's capabilities and contributions to a FoS or SoS.
- provide computerized representations of the system's human-machine interfaces to end-users to obtain final ergonomic modifications to the design (“Making design changes in the computerized representations will be much less costly than making the same changes in hardware prototypes.”)

- start training end-users on new systems.
- make final design trades and modifications before going into production.
- support transition to production with direct electronic transfer of digital system design data from the established collaborative to the manufacturing floor, “minimizing ambiguity in the systems specifications.”

M&S can be used during Production to (Section 4.5.7.4, DAG, 2006):

- define the production and support processes for the system (e.g., manufacturing facilities and production flows).
- start training end-users on new systems.

M&S can be used during Operations and Support to (Section 4.5.7.5, DAG, 2006):

- make design modifications that improve operational performance of a system and its effectiveness in an FoS or SoS construct, based on end-user innovation and feedback.
- incorporate end-user feedback and real world data to improve projections and examine redesign alternatives.

Though it is presented here as the last phase, Operations and Support may be considered the first phase of the acquisition cycle, since it is during this phase that new capability needs and requirements surface. Having gone through an iteration of the life cycle phases before it, the M&S for a system can be “re-used as course-of-action, decision support, and training tools” within a program, and additionally used as a representation of the system in other FoS and SoS M&S environments (Section 4.5.7.5, DAG, 2006). It is often during this phase of the lifecycle that architecture data is useful for Operational Planning, which is discussed in the next section.

5. Operational Planning

The DoDAF describes *Operational Planning* as the examination of “how various mission participants, systems, and information need to work together, to recognize potential problems that may be encountered, and to identify quick fixes that may be available to accomplish a mission” (Volume I, Section 3.1, DoDAF, 2007). As described in the previous section, M&S is a powerful tool that utilizes architecture data to inform such analyses. Certain views of architectural data can also be used directly to support mission planning by serving as a “script” for users to follow during mission training or execution, containing all the details and parameters of the information exchanges between participants and systems. Paired with M&S, the architectural data allows users to practice different potential variants of the mission. This is especially useful during the Operations and Support phase, as new capability needs emerge for exchanging data over systems that, earlier in their lifecycles, were not designed to operate efficiently as an SoS. Since the systems are already in place, needs for “quick fixes” to capability gaps surface. The needs are communicated through Joint Urgent Operational Needs (JUONs) (CJCSI 3470.01 Series, 2005), combatant commander’s integrated priority lists (IPL), lessons learned, and transitioning improvised explosive device (IED) initiatives (DoDD 2000.19E, 2006), which enter the JCIDS and acquisition processes at Milestone B or C upon approval by the Joint Requirements Oversight Council (JROC) (Enclosure A, Para. 1c, CJCSI 3170.01F, 2007).

Having architecture data in place that describes the present configuration in the deployed environment (or at any of the preceding stages of the system’s life) provides a basis for manipulation, simulation, and improvement of the system or SoS on an ongoing basis. Furthermore, data that is collected on the operation of deployed systems can be used to update the model of the architecture, adding a level of realism that enables operational planning activities such as mission bandwidth allocation, task reorganization, route optimization, and other predictive analyses.

F. CHAPTER SUMMARY

This chapter discussed the needs for and directives to develop integrated architectures in DoD; the architecture framework used for relating architectural data; features, and characteristics of integrated architectures; and various uses for integrated architectures referenced throughout the literature.

In addition to being mandated by federal law, architectures serve “to support strategic planning, transformation, and various types of analyses (i.e., gap, impact, risk) and the decisions made during each of those processes” (Volume I, Section 3.1, DoDAF, 2007). The takeaway from the detailed description of the uses of integrated architectures provided in this chapter is that the ultimate purpose of architecture data is to inform decision-supporting analyses, which are aimed at improving the system described in the architecture, in an iterative way, throughout its entire lifecycle.

Having established the purpose and context of integrated architectures throughout DoD policy and guidance, as well as their usefulness as data sets for informing various types of analyses and decision support, the next chapter presents an iterative systems engineering analysis process that utilizes integrated architectures.

III. THE RELATIONSHIP BETWEEN INTEGRATED ARCHITECTURES AND SYSTEMS ENGINEERING ANALYSIS

A. INTRODUCTION

This chapter builds on the previous chapter by defining Systems Engineering (SE) and SoS Engineering (SoSE), and describing how integrated architectures are used in the context of a systems engineering analysis process. Section B defines and describes systems engineering and its basis in DoD policy. Section C describes a systems engineering analysis process used by the Army Systems Engineering Office (ASEO) and its correlations with the DoDAF six-step architecture development process. Section D illustrates how the systems engineering analysis process described in Section C can be applied to the JCIDS process and Defense Acquisition Process. Section E summarizes the chapter.

B. SYSTEMS ENGINEERING IN DOD POLICIES AND GUIDES

The systems engineering analysis process described in the following section has roots in DoD policy and guidance. In 2004, the Under Secretary of Defense Acquisition, Technology & Logistics (USD AT&L) issued a Policy for Systems Engineering in DoD to “drive good systems engineering processes and practices back into the way we do business.” It states that “Application of rigorous systems engineering discipline is paramount to the Department’s ability to meet the challenge of developing and maintaining needed warfighting capability. This is especially true as we strive to integrate complex systems in a family-of-systems, system-of-systems, net-centric warfare context. Systems engineering provides the integrating technical processes to define and balance system performance, cost, schedule, and risk. It must be embedded in program planning and performed across the entire acquisition lifecycle.” The policy requires that “All programs responding to a capabilities or requirements document, regardless of the acquisition category, shall apply a robust SE approach that balances total system performance and total ownership costs within the family-of-systems, system-of-systems context," and that the programs develop a Systems Engineering Plan (SEP) that describes the program's overall technical approach (to include processes, resources, metrics, and applicable performance incentives) as well as the timing, conduct, and success criteria of technical reviews. The policy addendum (22 Oct 2004) mandates that each Program Executive Officer (PEO) or equivalent have a lead or chief systems engineer on his or her staff responsible to the PEO for applying systems engineering across the PEO's portfolio of programs. The addendum also endorses the systems engineering best practices provided in the Defense Acquisition Guidebook.

Systems engineering is referenced once in each of the JCIDS documents. The JCIDS instruction states that "The process to identify capability gaps and potential materiel and non-materiel solutions must be supported by a robust analytical process that objectively considers a range of operating, maintenance, sustainment, and acquisition approaches and incorporates innovative practices -- including best commercial practices, HSI [Human Systems Integration], systems engineering (including safety and software engineering), collaborative environments, modeling and simulation, and electronic business solutions" (Enclosure B, Para. 3, CJCSI 3170.01F, 2007). The JCIDS manual's CDD format guide (Appendix A to Enclosure F, CJCSM 3170.01C, 2007) requires that system attributes be presented in measurable and testable terms, each with a threshold and an objective value. It explains that "Expressing capabilities in this manner enables the systems engineering process to develop an optimal product." Note that the systems engineering process both supports and is enabled by the processes in the JCIDS.

The next section discusses a "robust analytical process" as described in the JCIDS reference for conducting systems engineering analysis using the "innovative practices" mentioned. Before delving into the mechanics of this process, however, it is necessary to define "systems engineering," "system of systems engineering" and "systems engineering analysis." These definitions will provide a context for the description of the use of integrated architectures to support systems engineering analyses.

The term *systems engineering*, like the terms *system* and *System of Systems* provided in Chapter I, has no single globally accepted definition. The following definitions are three representative perspectives, the first from the International Council on Systems Engineering (INCOSE), the second from the Defense Acquisition Guidebook, and the third from the Naval Postgraduate School.

- "Systems Engineering is an interdisciplinary approach and means to enable the realization of successful systems. It focuses on defining customer needs and required functionality early in the development cycle, documenting requirements, and then proceeding with design synthesis and system validation while considering the complete problem. Systems Engineering considers both the business and the technical needs of all customers with the goal of providing a quality product that meets the user needs." (INCOSE SE Handbook v3, 2006)
- "Systems engineering is the overarching process that a program team applies to transition from a stated capability need to an operationally effective and suitable system. Systems engineering encompasses the application of systems engineering processes across the acquisition life cycle (adapted to each and every phase) and is intended to be the integrating mechanism for balanced solutions addressing capability needs, design considerations and constraints, as well as limitations imposed by technology, budget, and schedule. The systems engineering processes are applied early in concept definition, and then continuously throughout the total life cycle." (Section 4.1, DAG, 2006)
- "Systems Engineering is the profession in which knowledge of multiple disciplines gained by study, experience, and practice is applied in a structured, iterative manner with judgment to identify and solve problems and deliver results expected by stakeholders." (Langford on Systems Engineering, 2007)

The last definition above, from the Naval Postgraduate School, is best suited to the discussion in this chapter since the process presented is structured and iterative, and is used to identify and solve problems and deliver results to stakeholders.

Just as the concept of a System of Systems has followed that of a single system, the concept of System of Systems Engineering has followed that of systems engineering. System of Systems Engineering (SoSE) "deals with planning, analyzing, organizing, and integrating the capabilities of a mix of existing and new systems into a system of systems capability greater than the sum of the capabilities of the constituent parts." Conducting SoSE is more complex than conducting SE because "the development of a system of systems solution will involve trade space between the systems as well as within an individual system's performance" (Section 4.2.6, DAG, 2006).

SoSE emphasizes "discovering, developing, and implementing standards that promote interoperability among systems developed via different sponsorship, management, and primary acquisition processes" (p. 53, Guide to SoSE, 2006). Thus, there is a level of interoperability at the SoS level that is distinct from, above and beyond interoperability at the systems level. Interoperability must include organizational considerations if the constituent systems are not under the control of one SoS owner. Organizations that own the constituent systems must collaborate in order to develop a successful SoS. Furthermore, the SoS itself will attract more stakeholders that are not part of any of the constituent systems due to the possibility that components of the SoS are part of other SoS (p. 10, Guide to SoSE, 2006), and the emergent capability of the SoS (which is greater than the sum of the capabilities of the constituent parts). The addition of these stakeholders is the essence of the difference between organizational collaboration at the systems level and organizational collaboration at the SoS level.

Such complex organizational interactions require governance and collaboration. *Governance* is defined in the SoSE Guide as "the processes and systems by which an organization and system operates, the rules of engagement, the escalation mechanisms, the change management and conflict resolution mechanisms, and the enforcement mechanisms." Establishing a Governance Architecture is cited as one of the four pragmatic challenges for the effective synthesis and deployment of SoS. Governance Architecture comprises

“Institutions, structures of authority and collaboration to allocate resources and coordinate or control activity. A governance architecture is critical to the synchronized and effective management and integration of multiple, independent programs and systems into a system of systems” (p. 5, Guide to SoSE, 2006). The concept of a governance architecture is discussed further in Chapter IV.

Finally, *systems engineering analysis* is defined as any structured, iterative, multi-disciplinary analysis that uses measures of merit to identify and solve problems and deliver results expected by stakeholders (based on Langford on Systems Engineering, 2007).

The DAG states that “Systems of systems should be treated and managed as a system in their own right, and should therefore be subject to the same systems engineering processes and best practices as applied to individual systems” (Section 4.2.6). Therefore, the systems engineering analysis process described in the next section is also applicable to SoS engineering analysis.

C. SYSTEMS ENGINEERING ANALYSIS PROCESS

This section discusses the process that the ASEO uses to conduct quick reaction systems engineering analysis. “Quick reaction” refers to the type of analysis typically conducted during the Operations & Support phase, to evaluate problems occurring in deployed systems, and has a timeline of weeks to months associated with it. This process is an adaptation of the Systems Analysis Process diagram in Blanchard and Fabrycky’s Systems Engineering and Analysis text (Figure 4.9, p. 112, Blanchard & Fabrycky, 2006). The process is refined continuously through experience gained from and lessons learned in iterating the process. In addition to its ability to be scaled up for application throughout an acquisition system’s lifecycle (as illustrated in Section D), this analysis process is general enough in concept to be customizable to just about any type of analysis problem, from building or remodeling a house to conducting major force structure reorganizations. This section discusses how the process has been customized for the development, analysis and iterative improvement of integrated architectures in support of quick reaction analyses.

This systems engineering analysis process correlates to and extends the six-step process of building an architecture description detailed in Section 2.2 of DoDAF Version 1.5 Volume I (Figure 8). The two processes generally run in parallel with one another, and it is possible (though not desirable, as will be discussed) to execute one process independently of the other. In other words, it is possible to do a systems engineering analysis on a data set that does not meet the criteria of an integrated architecture, and it is possible to develop an integrated architecture without subjecting it to a systems engineering analysis process. However, the quality of products resulting from the two processes done independently will be substantially lower than the quality of products resulting from the integral coordination of these two processes. As is discussed in the paragraphs below, integrated architectures provide highly detailed sets of source data for use in conducting systems engineering analyses, and in turn, the systems engineering analysis results and conclusions aid in the improvement of these integrated architectures resulting in a better product for the warfighter.

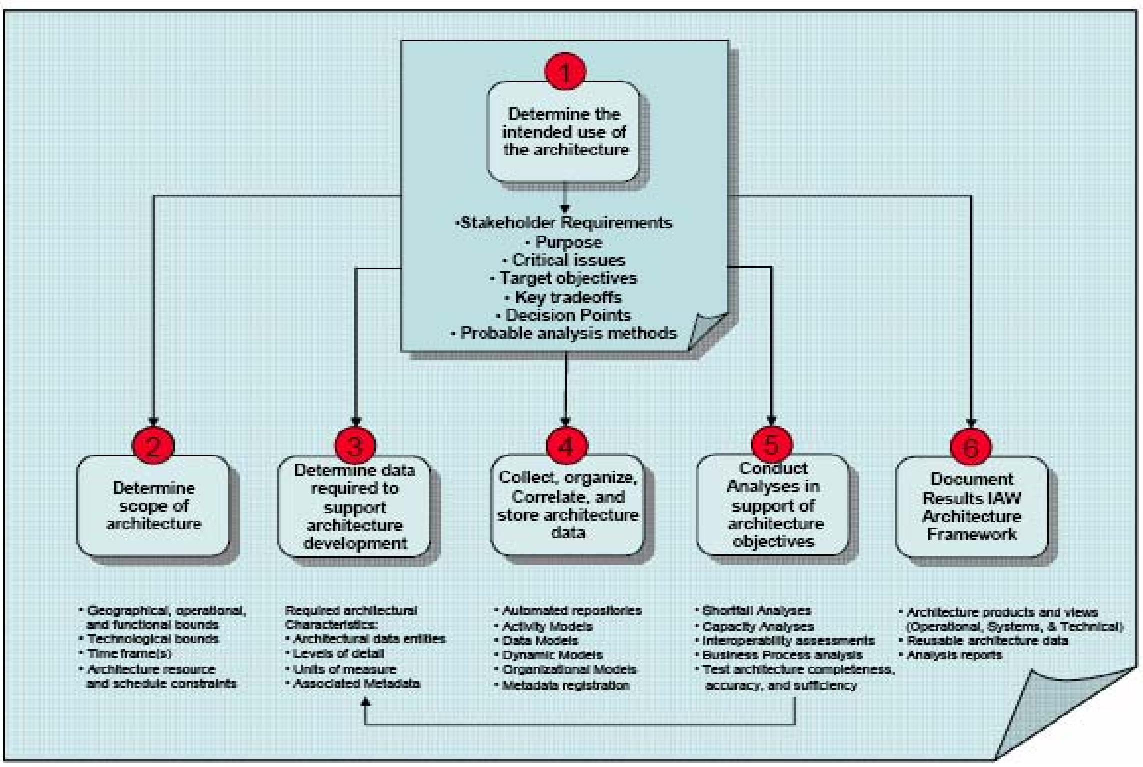


Figure 8 The Six-Step Process of Building an Architecture Description (From: Figure 2-1 in Volume I, DoDAF, 2007)

An overview of the ASEO systems engineering analysis process is shown in Figure 9. The process described herein is customized to the “quick reaction” timeline, omitting some steps that would be important to include when applying this process to an acquisition program over the course of the lifecycle, such as lifecycle impacts, Test & Evaluation (T&E) requirements and execution, and Verification & Validation (V&V) of assessment criteria. The numbered red circles represent the architecture development steps from Figure 8, and serve as a visual reference to general correspondences between the architecture process steps and the systems engineering analysis process steps.

The following paragraphs provide a description of each of the systems engineering analysis process steps and the DoDAF architecture development process steps in parallel. The purpose of the comparison is to highlight generally similar activities in each process, and to enable readers who are familiar with one process to relate to the other and see the connections and opportunities for integration of the two processes. More work is needed to conduct a full comparison and integration of the two processes, and evaluate the consequences of continuing to perform the processes independently of one another.

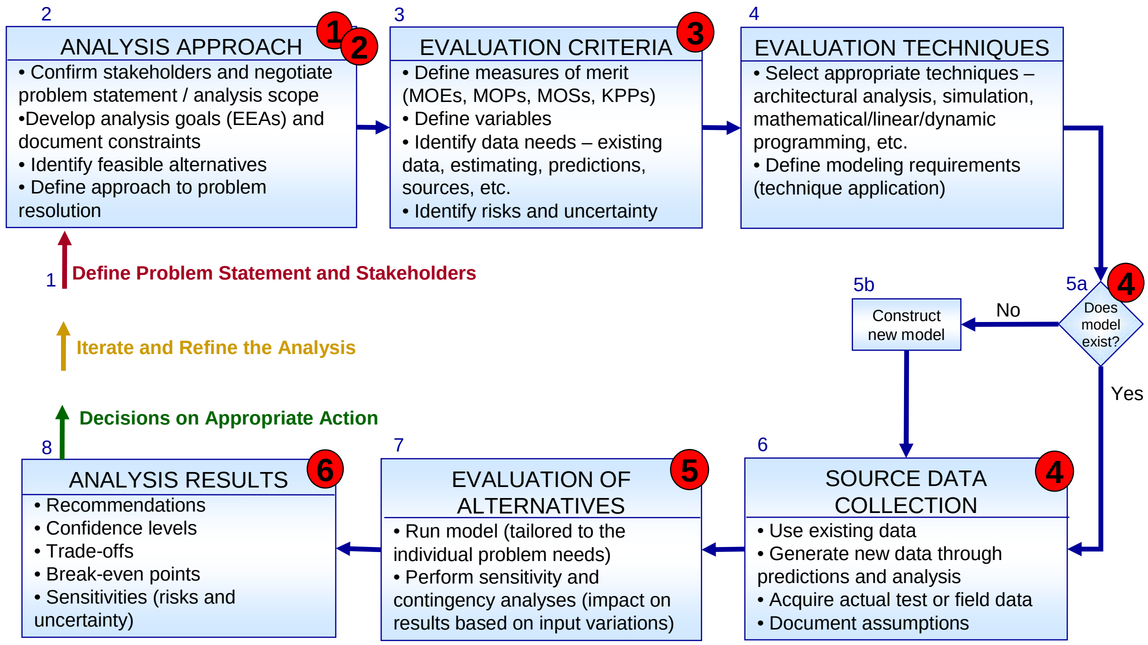


Figure 9 ASEO Systems Engineering Analysis Process.

1. Define Problem(s) and Stakeholders

The systems engineering analysis process always begins with identifying the problem(s) to be analyzed. Step 1 of the quick reaction analysis process consists of the analysis team receiving a problem statement and an initial list of stakeholders concerned with the analysis.

The initial problem statement and list of stakeholders are initial inputs to the process. Once it has been confirmed that there is a need to solve the problem, the systems engineering analysis process continues onto the next step to refine and reiterate the problem statement, confirm all important stakeholders have been coordinated with, and determine the analysis scope and approach.

2. Analysis Approach

Very often, the analysis approach is dependent on the problem being assessed. The problem that is assessed depends on the scope of analysis, the priority of analysis questions, constraints of the analysis, and system boundaries depend on the individuals and organizations that have a stake in the problem (and its potential solutions) and the way these stakeholders' needs are included and prioritized. This step addresses these issues.

<u>Confirm stakeholders and negotiate problem statement / analysis scope.</u> The analysis team must establish communications with all relevant stakeholders, and coordinate a review, reiteration, and negotiation of the problem statement among the stakeholders in order to establish the analysis scope, a prioritized list of analysis questions, constraints, system boundaries, and an analysis approach appropriate to the resultant problem definition. The problem statement must be coordinated, discussed, negotiated and refined with all relevant stakeholders. Refinement of the problem often involves identification of more stakeholders. Early identification of stakeholders is critical to avoid substantial needs being overlooked in attempting to solve a problem in an optimal way. In large-scale system of systems problems with multiple competing objectives, an optimal solution for one stakeholder often degrades the solution for other stakeholders. For example, one group of stakeholders may be most concerned about having enough bandwidth (kilobits per second), while another group may be most concerned about keeping down cost (dollars). Multiple objectives must be taken into account so that the solution to the problem does not result in an unacceptable outcome for one or more of the stakeholders. Limiting the number of stakeholders may shorten negotiations and save time and effort in conducting the analysis, however doing so may have serious foreseeable consequences that should be considered up front. By doing so, the analysis results can describe the impact (if not an optimal result) on all factors that are important to all stakeholders so that the consequences of implementation decisions are understood by all.

The analysts must ensure that a pure problem statement is defined, so that potential explanations or solutions are not inadvertently written into the problem definition, which can cause other potential solutions to be overlooked. The analysts must sometimes help the stakeholder(s) produce a problem statement that can be decomposed into elements of analysis.

In addition to helping refine the problem statement and analysis scope, stakeholders participate throughout the process by providing potential courses of action (feasible alternatives), source data, information required to build models, and feedback on initial analysis results. Although not graphically represented in Figure 9 for simplicity, feedback loops run back to the stakeholders from every step in the process.

The final list of stakeholders, problem statement, and analysis scope is coordinated with the sponsor and other stakeholders prior to continuing the analysis.

<u>Develop Essential Elements of Analysis (EEAs) and document constraints.</u> Specific analysis questions are then developed or derived from the problem statement, if this has not yet been done in the course of negotiations. As stated previously, the types of analysis questions can vary. Some examples of quick reaction analysis questions for a given application, network, or mission thread are:

- Does the IT architecture describe an interoperable set up (i.e., can systems and people communicate as required)?
- What is the end-to-end response time (e.g., from information requested / passed to information received / acted upon)?
- What is the impact of increased network traffic on bandwidth?
- How can communications elements be arranged at the lower layers to support the efficient exchange of application-level traffic?
- What is the impact on the network (or user, or mission) when critical routing elements are taken out of service?
- How does force structure reorganization affect network reconvergence?
- What is the impact when a new system or new version of a system is added to the SoS?
- Will the proposed communications architecture support real-time applications (e.g., voice, video)?

Once the analysis questions have been coordinated with the stakeholders, they are documented as Essential Elements of Analysis (EEAs).

At this time, additional general or specific limitations or constraints imposed on the analysis are documented. These constraints may pertain to the general scope of the analysis, result from very specific impositions of one or more stakeholders, result from organizational issues or policy, or take the form of assumptions made in the absence of reliable information. Constraints may be general statements, or be expressed mathematically (usually with inequalities, such as a certain measure must be less than or equal to some value).

EEAs and constraints are always reiterated back to the sponsor and other stakeholders along with the problem statement, before the analysis gets underway. This reiteration of objectives is necessary in order to confirm that the right questions are addressed in the analysis, and that no available information has been overlooked by the analysts.

Identify the premise or feasible alternatives. In less complex problems with a limited number of possible solutions, stakeholders sometimes have either a single premise or several feasible alternatives in mind, but are unsure whether the premise is valid or, if alternatives are being considered, with which course of action (COA) to proceed. When a premise is proposed, the objective of the analysis is to determine the validity of the premise (i.e., a confidence study). When a finite number of COAs are being considered for implementation, the objective of the analysis is to determine which COA provides the maximum benefit. Information on each potential COA is collected and added to the analysis documentation at that time. This step does not take place up front for analyses that have an unbounded number of potential solutions.

Define approach to problem resolution. Once the problem, EEAs, constraints, and potential alternatives have been identified, the final activity in this step is to consider the general approach to addressing the problem. Given the nature of the problem, the analysts make a determination on the specific methodology and associated level of effort required to conduct the analysis. For example, the analysts may investigate whether the questions can be addressed with a simple information gathering and study, or more rigorous and sophisticated techniques such as bandwidth, performance, or risk analyses are required. Best and worst case estimates for the analysis schedule and time to initial results are made.

There is some correlation between the activities of Steps 1 and 2 of the systems engineering analysis process and the activities in Steps 1 and 2 of the architecture development process, which describes initiation activities of an architecture project. “Step 1: Determine Intended Use of Architecture” entails explaining why the architecture is being developed, what the architecture will accomplish, and how it may affect organizations or systems; and establishing clear and concise exit criteria for measuring customer satisfaction in meeting overall requirements with the architecture. This step also entails the development and approval of the purpose section of the AV-1 (Volume 1, Section 2.2, DoDAF, 2007). “Step 2: Determine Scope of Architecture” involves establishing boundaries for the depth and breadth of the architecture and the architecture’s problem set, as well as helping to define its context (e.g., environment, organizational mission and vision, subject area, time frame, and intended users). This step also entails the development and approval of the purpose section of the AV-1. Stakeholder coordination is not explicitly described either of these steps, though it is implied in determining how the architecture “may affect organizations and systems” and defining its context (“environment, organizational mission and vision, subject area, time frame and intended users”).

3. Evaluation Criteria

<u>Define measures of merit.</u> The evaluation criteria are determined by defining specific measures that will be used in a quantitative analysis. While EEAs are sufficient for conducting a literature-based analysis, EEAs alone are not sufficient for conducting a quantitative analysis. More specific target questions must be determined in order to have measurements to support conclusions to the EEAs in a quantitative analysis. The EEAs are therefore decomposed into more specific measures, known as Measures of Effectiveness (MOEs), Measures of Performance (MOPs), and Measures of Suitability (MOSs).

A Measure of Effectiveness is defined in the *DAU Glossary of Defense Acronyms and Terms, 12th Edition* (DAU Online Glossary, http://acquire.dau.mil/jsp/Glossary.jsp) as a “measure designed to correspond to accomplishment of mission objectives and achievement of desired results.” Measures of Effectiveness may be decomposed into Measures of Performance and Measures of Suitability. A Measure of Performance is defined as a “measure of a system’s performance expressed as speed, payload, range, time on station, frequency, or other distinctly quantifiable performance features” (DAU Glossary). A Measure of Suitability is a “measure of an item’s ability to be supported in its intended operational environment. MOSs typically relate to readiness or operational availability, and hence reliability, maintainability, and the item’s support structure” (DAU Online Glossary). These MOEs, MOPs and MOSs should trace back to Key Performance Parameters (KPPs), “those attributes or characteristics of a system that are considered critical or essential to the development of an effective military capability,” and “are included verbatim in the Acquisition Program Baseline (APB)” (DAU Glossary).

Define variables. Once the EEAs, MOEs and MOPs are defined, the variables in the analysis are defined. There are two basic types of variables: independent (controllable) and dependent (uncontrollable). Independent variables can be specified in the design or configuration of the system, whereas dependent variables are generally measured outcomes.

Identify data needs. In order to obtain credible and realistic results, certain types of information and data (hereafter referred to simply as “data” unless otherwise noted) must be gathered to populate the model. The data may already exist (i.e., historical data), be calculated estimates (i.e., predictions), or be a combination of the two (i.e., predictions based on historical data augmented with new information and/or assumptions). The types of data needed vary, depending on the analysis being conducted. Along with the types of data, potential sources are identified and a data call is prepared. The data call is then distributed to the stakeholders who are potential sources for the data or information required to do the analysis. In order to receive timely, accurate and complete feedback on the data call, especially when the analysis concerns an SoS with multiple organizations involved, it is important to do the following:

- Identify points of contact (POCs) who either have the information or know where to get it
- Establish introductions and communicate the data requirements to these POCs
- Establish trust between providers and requesters of the data call that the data or products shared (which are often “draft”) will not be misused, assessed prematurely for completeness/accuracy if they are works in progress, or otherwise be the subject of destructive criticism
- Clearly state the benefits of the most timely, accurate and complete response possible, especially explaining the value to the provider. In other words, explain how providing this information or data will eventually help them do their jobs better. Follow up by recognizing data providers for their contributions by giving them credit as they provide data, and acknowledge their support again in the analysis deliverables.

If a thorough job of identifying and communicating with stakeholders was done in Step 2, the above four steps of the data call process should be relatively straightforward. However, in SoS, involvement of stakeholders is often dynamic (p. 10, Guide to SoSE, 2006) and new stakeholders are identified during the data call process. Additional effort will be required to explain who is requesting the data, what it will be used for, and why their response is important. In either case, it is easy for precious weeks, even months, to slip by while waiting for these steps to take place. It is critical that the data requesters monitor progress very closely to prevent schedule slips.

Identify risks and uncertainty. Risks identified may be associated with management of the project (e.g., cost, schedule, performance) or with the technical execution of the project (e.g., technical data not available, accurate, or stable). Key variables (uncertainties) that have a significant bearing on the outcome must be identified and minimized, since a large swing in the values for these variables may result in a different set of recommendations. The greater and more numerous the uncertainties, the greater the risks of providing inaccurate results and, consequently, recommendations that are off the mark.

There is some correlation between this step of the systems engineering analysis process and the activities in Step 3 of the architecture development process. "Step 3: Determine Data Required to Support Architecture Development" involves selecting operational, systems and services, and technical standards view data entities, attributes, and rules based on input from the process owner. The required level of detail for the data to be captured is specified during this step, and this information guides the data collection effort pertaining to the architecture structure in "Step 4" of the architecture development process (Volume 1, Section 2.2, DoDAF, 2007). However, there is no explicit mention of defining measures of merit that can be used to quantify success at meeting requirements.

4. Evaluation Techniques

Select appropriate techniques. Given the MOEs, MOPs, and MOSs, evaluation techniques are reviewed and selected for application to the analysis problem. The evaluation technique selected should provide results that address the measures with a granularity and fidelity appropriate to the analysis problem, and the limitations of the technique should be understood and documented as necessary. Four general analysis techniques are summarized below in the context of integrated architecture analysis: literature review; architectural data analysis; operational, systems and/or technical architecture analysis; and system optimization analysis.

The most basic technique is the *literature review*, which investigates whether the analysis problem has been addressed previously or if the answer is otherwise attainable without employing a more detailed analysis technique. A literature review is conducted to gather all available information on a particular topic. Conducting a literature review often prevents duplication of work and unnecessary expenditure of resources on previously or concurrently addressed topics, and should be a precursor to any other analysis technique to gather all the pertinent information and data on a particular problem that is available.

Architectural data analysis is another technique that is used when the analysis problem concerns the quality and integrity of the architecture itself. This is a quality control type of analysis where the analyst ensures that the data in the architecture meets certain criteria for being certified as an integrated architecture (see the “Features of Integrated Architectures” section in Chapter II), and ensures that the architecture data has integrity in the sense that there are no overt gaps in the architecture data (e.g., an operational node with no systems assigned, a system function that does not trace back to some operational function, etc.). Analysis of the quality of the architecture data is a prerequisite to analysis of the quality of the design described by the architecture data, which is described next.

Operational, systems, and/or technical architecture analysis may be conducted directly by evaluating the architecture products in and of themselves to determine, to the degree possible without more sophisticated techniques, the quality of the design described by the architecture data. This type of analysis is most effective when the architecture is integrated and has already undergone a quality control analysis described above. Models (defined and described in Chapter II) are employed and navigated to understand and evaluate the configuration of the integrated architecture. Examples of this type of analysis include verifying that the required systems are associated with the operational nodes that must communicate, and the required technical standards are associated with systems that must communicate. This type of analysis ensures, at a minimum, that the integrated architecture describes a feasible solution.

System optimization analysis is the final category of evaluation techniques and consists of the most advanced methods and tools for answering difficult analysis questions. Modeling and simulation (M&S) is a primary enabler for system optimization. The reader is referred to Chapter II for a detailed discussion of M&S and its applications to addressing analysis questions throughout the system lifecycle, all of which are applicable in the systems engineering analysis process. A science that extensively uses M&S to solve mathematical problems is Operations Research (OR). OR “is the development and application of mathematical models, statistical analyses, simulations, analytical reasoning and common sense to the understanding and improvement of real-world operations. Improvement can be measured by the minimization of cost, maximization of efficiency, or optimization of other relevant measures of effectiveness." The military applies OR at strategic, operational, and tactical levels to improve decision making and facilitate insights into the phenomena of combat (NPS Graduate School of Information Sciences, 2007). Another technique that may be used in system optimization is *emulation*, in which a program or device exactly replicates the behavior of another program or device. Emulation differs from simulation in that emulation replicates behavior exactly, whereas simulation uses an abstract model of the system being simulated, focusing on key characteristics and behaviors and the use of simplifying approximations and assumptions.

Define modeling requirements. For those analyses employing models, hardware, software, and data requirements are specified to represent the behavior of systems or components that are part of the system undergoing analysis. For example, when modeling an IT network, the behavior of the relevant application, transport, network, data link, and physical layer devices must be described.

There is no correlation between this step and any of the six DoDAF architecture development process steps since the determination of evaluation techniques are not explicitly discussed in any of the DoDAF architecture development process steps.

5. Obtain, Construct and/or V&V Models

If models are to be used in the analysis, it is recommended that a search for existing models be conducted before model development begins, in order to benefit from previous work done and ultimately save time and resources. Often, models developed during previous analyses can be reused with minor changes. When the necessary models do not exist, they must be constructed and undergo

Verification and Validation (V&V) to ensure that the models are both complete (the model captures all the necessary relationships) and convincing (the model produces repeatable and persistent results).

In order to develop and/or configure the necessary models, input requirements and conditional statements must be expressed. Modeling requirements can be expressed in different ways, depending on the type of analysis. For example, they may be expressed in terms of a simulation run matrix, or as a linear programming (LP) model formulation employing OR techniques. A simulation run matrix explicitly states the combinations of values for the controllable variables that will be simulated. This method can be used when a limited number of COAs are being considered due to non-technical constraints. A linear program formulation does not explicitly state values for decision variables, or combinations thereof. Instead, the LP formulation employs the computational power of a solver to calculate precise values for controllable variables, given a set of constraints (inequalities that bound the uncontrollable variables).

Model construction and/or V&V may occur in parallel with the next step, source data collection. Obtaining, constructing, and/or V&V of models, per se, are not explicitly discussed in the DoDAF architecture development process. However, per the description of architecture products and models provided in Chapter II, architecture products *are* schematic models. Therefore, the activities of this step of the systems engineering analysis process may correlate with the activities in "Step 4: Collect, Organize, Correlate, and Store Architecture Data" of the architecture development process. Step 4 is discussed in more detail at the end of the next section.

6. Source Data Collection

Following or in parallel with Step 5, source data is collected for use in the analysis. This step typically begins with the review of data received as a result of the data call initiated during "Identify data needs" in Step 3. As discussed, this data may be historical (acquired from actual test, experiment, or operations data), predictive (generated via calculated estimates, modeling and simulation, or subject matter expert advisement), or a combination of the two. Regardless of the data sources, an essential part of the systems engineering analysis process is the documentation of where all data came from (sources and references), as well as all assumptions, caveats, and constraints associated with the data. This documentation is essential for traceability, should the validity of the data upon which the analysis is based be called into question. Having this documentation readily accessible helps consumers of the analysis understand the context in which the analysis was conducted, and enables corrections and modifications to assumptions that might very well result in a different set of conclusions and recommendations.

If this is the first iteration of the overall process for a given set of EEAs and their associated measures, and an integrated architecture does not exist, source data collection is the most lengthy and time-consuming step in the systems engineering analysis process. The following steps occur during source data collection:

- Electronically or physically transport the data from the provider to the analyst. This can be challenging if the files are large, numerous, access-restricted, and/or classified.
- Verify that the files contain the data required to conduct the analysis.
- If an integrated architecture does not exist, compile and synthesize data received from multiple sources into one source data repository, and populate the appropriate architecture products. This step often takes place for systems that bypass the Defense Acquisition Process and are deployed immediately to satisfy an urgent operational need. A highly customized, “mini” integrated architecture must often be assembled from the provided data at an appropriate scope to address the specific measures of the analysis. This step has two sub-steps:
    - Make the appropriate mappings among the various elements of source data. For example, one document may contain the force structure, another the network laydown, another the dispositions of the systems of interest, another the physical routes, and yet another the usage patterns of the systems of interest. These files are not necessarily formal DoDAF

products and may not even necessarily exist. The analyst may be required to collect data, either directly from the network or by interviewing operators to determine usage patterns for certain applications, for instance.

    - Resolve ambiguous or conflicting entries. For example, the same entity may have two different names in two documents from different authors, apparent duplicates or holes in the data, and/or information in one document that otherwise contradicts information in another. This is an architectural data analysis as described in Step 4 of the systems engineering analysis process, and is necessary to complete before the data can be used for other, more complex types of analyses.

- Sanitize the data, if the analysis environment is at a lower classification level than the data. ASEO's process involves reviewing the security classification guides pertaining to each system and network in the source data repository, removing classified and sensitive information, marking and formatting the data file for printing, printing off the data file, conducting an additional security review of the printed pages, removing the printed pages from the classified environment, scanning the pages into a computer in the unclassified environment, bringing an electronic copy of the sanitized version back into the classified analysis environment to manually correct scanning errors, and outputting a sanitized and corrected version of the data file.

Conducting all of the above steps is not a trivial task, especially under the time constraints of a quick reaction analysis. These time consuming activities must take place before a rigorous evaluation of alternatives can begin. The following steps can be taken, where possible, to maximize efficiency of conducting the source data collection step of the analysis process:

- Early establishment of mechanisms for electronically or physically transporting data and information between provider and analyst.
- Establish good relationships between data providers and analysts, as detailed in “Identify data needs,” to maximize timeliness, accuracy and completeness of the data required to conduct the analysis.
- Have an integrated architecture (or elements thereof) readily available for use to reduce or eliminate the need to compile and synthesize data in preparation for the analysis .

- When available, conduct analysis of classified data in a classified analysis environment, and sanitize the analysis results (if necessary) rather than the source data.

The key recommendation in the context of this thesis is c., Have an integrated architecture available to the systems engineering analysis process. In the absence of integrated architectures, assembly of the tailored data set in Step 6. iii. by analysts is often necessary due to the timeframe in which the analysis questions are due to be answered. As a consequence, architecture formality is foregone in these quick turn analyses. The underlying data set used in the analyses is highly specific to the systems and system attributes of the analysis, and most likely not compliant with DoDAF and CADM. These features limit the reuse possibilities, despite the enormous effort of assembling the information. The data set becomes irrelevant as time passes if it is not placed into an integrated architecture under configuration control and maintained throughout the lifecycle. The lack of access to such an integrated architecture significantly lengthens the amount of time needed to collect, integrate, use, update, and *reuse* the data required for analysis throughout a system's life. Thus, the need for integrated architectures is further justified by their use not only as foundational data sets for informing analysis questions, but for capturing improvements to the design identified as a direct result of iterative systems engineering analyses.

There is a strong correlation between the activities of this step of the systems engineering analysis process and the activities in Step 4 of the architecture development process. "Step 4: Collect, Organize, Correlate, and Store Architecture Data" involves locating and reusing published and accessible architecture content from other DoD sources, when possible; capitalizing on taxonomies of standardized reference data; and cataloguing, organizing, and correlating the architecture data into automated repositories to permit subsequent analysis and reuse. The DoD Architecture Registry System (DARS) is to be used to discover and review architecture content, and register metadata about the architecture under development as soon as it is available to support discovery and enable federation (Volume 1, Section 2.2, DoDAF, 2007). This strong correlation makes sense, since architecture data directly supports systems engineering analyses.

7. Evaluation of Alternatives

After being collected and integrated, the source data is then ready for the next step, evaluation of alternatives. If there is a single proposed COA or premise, the alternatives evaluated consist of a qualified go or no-go for that COA or premise. If there is more than one alternative, the alternatives are evaluated against one another. If a model is used, source data is formatted and inputted into the specific analysis tool(s) (e.g., solvers and simulators) being used to conduct the analysis.

Run model. Executable models and simulations are run to determine optimal values for the variables. The results must be analyzed in the context of the analysis questions. If the solution is not acceptable, the constraints or input data can be revisited and the models rerun iteratively until an acceptable solution set is determined. Specifically, values of controllable input variables may be adjusted in the model, and/or values of controllable variables linked to constraints (boundary conditions) may be adjusted to make constraints elastic.

Perform sensitivity and contingency analyses. Sensitivity analysis can be conducted to determine the effect of changing a variable (or set of variables) over a specific range of values on the analysis results. Sensitivity analysis is a "procedure to determine the sensitivity of the outcomes of an alternative to changes in its parameters… If a small change in a parameter results in relatively large changes in the outcomes, the outcomes are said to be sensitive to that parameter. This may mean that the parameter has to be determined very accurately or that the alternative has to be redesigned for low sensitivity." A contingency analysis "explores the effect on the alternatives of change in the environment in which the alternatives are to function. This is a "what-if" type of analysis, with the what-ifs being external to the alternative, in contrast to a sensitivity analysis, where the parameters of the alternatives are varied" (Heylighen, 2007).

There is a correlation between the activities of this step of the systems engineering analysis process and the activities in Step 5 of the architecture development process. "Step 5: Conduct Analysis in Support of Architecture Objectives" entails analyzing the architecture data to determine its effectiveness in supporting the initial process owner requirements. The outputs of this step are the architecture for approval, and the identification of additional data required to complete the architecture and "better facilitate its intended use through iteration of the architecture process" (repeating steps 3 through 5) (Volume I, Section 2.2, DoDAF, 2007). However, the methods of analyses are not discussed and the analysis rigor required to validate that the architecture meets requirements is not specified. The lack of discussion on rigorous analysis is consistent with the lack of definition of measures of merit.

8. Results and Recommendations

The results of the modeling and other analyses are studied and documented in the context of the problem statement, analysis questions, EEAs, and measures; and conclusions about the results are drawn. One type of conclusion is that the results indicate a high level of confidence in the validity of the premise, or in one or more of the proposed COAs. This type of conclusion provides the analysis-based validation of COAs that are required by customers to make confident decisions. Conclusions can also be made with respect to potential trade-offs between several efficient solutions. The alternatives are presented to decision makers, along with information that can be used to support the decision. Break-even points address the points at which benefits gained by implementing one COA exceed the drawbacks and vice versa, based on specific variables of interest. Sensitivities in variables of interest are documented and presented to leadership, particularly when these variables have values to which slight changes may result in extremely different outcomes (those that can potentially “flip” the recommendations). Finally, based on the conclusions, specific recommendations are made to support decisions on the appropriate actions. After the results and recommendations have been coordinated with the stakeholders, the analysis products are released for wider distribution.

There is a correlation between the activities of this step of the systems engineering analysis process and the activities in Step 6 of the architecture development process. In the context of a systems engineering analysis, the views that are rendered represent the recommended architecture configuration. The DoDAF process “Step 6: Document Results in Accordance with Architecture Framework” involves rendering the architecture products from the underlying data for presentation to the intended audiences. The renderings may be standard DoDAF products or user-defined custom products that are reusable, shareable, and include the underlying data (Volume I, Section 2.2, DoDAF, 2007). However, there is no mention of analysis or other supporting products that accompany, explain and caveat the rendered architecture views.

9. Iterate and Refine the Analysis

Feedback on the analysis results can generate more analysis questions, more variables, or different values for variables that decision makers want to see modeled. In this case, all or part of the process is repeated, making the requested modifications to the original source data and/or models. For each subsequent iteration, the analysis takes much less time since the bulk of the data was already put in place during the first iteration, especially if the analysis process has access to an integrated architecture.

There is a weak correlation between this step of the systems engineering analysis process and Step 6 of the architecture development process, in that the latter step mentions reuse of the architecture products. However, the DoDAF process step does not explicitly mention iteration and refinement based on any analysis and findings resulting from the architecture effort.

D. APPLICABILITY TO THE JCIDS AND DEFENSE ACQUISITION PROCESSES

The analysis process presented in the previous section is scaleable for application throughout the acquisition lifecycle, from Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel and Facilities (DOTMLPF) analysis and the JCIDS process through the Operations and Support phase. Systems engineering analyses take place throughout the lifecycle, though the analysis topics or questions being asked may vary from phase to phase. The results and recommendations of these analyses can inform decision points throughout the acquisition process. Figure 10 and Figure 11 illustrate various decision points in the acquisition lifecycle that are informed by systems engineering analyses. The concept of the application of the process throughout the acquisition lifecycle is graphically depicted in Figure 12 using Figure 11 as a foundation[1].

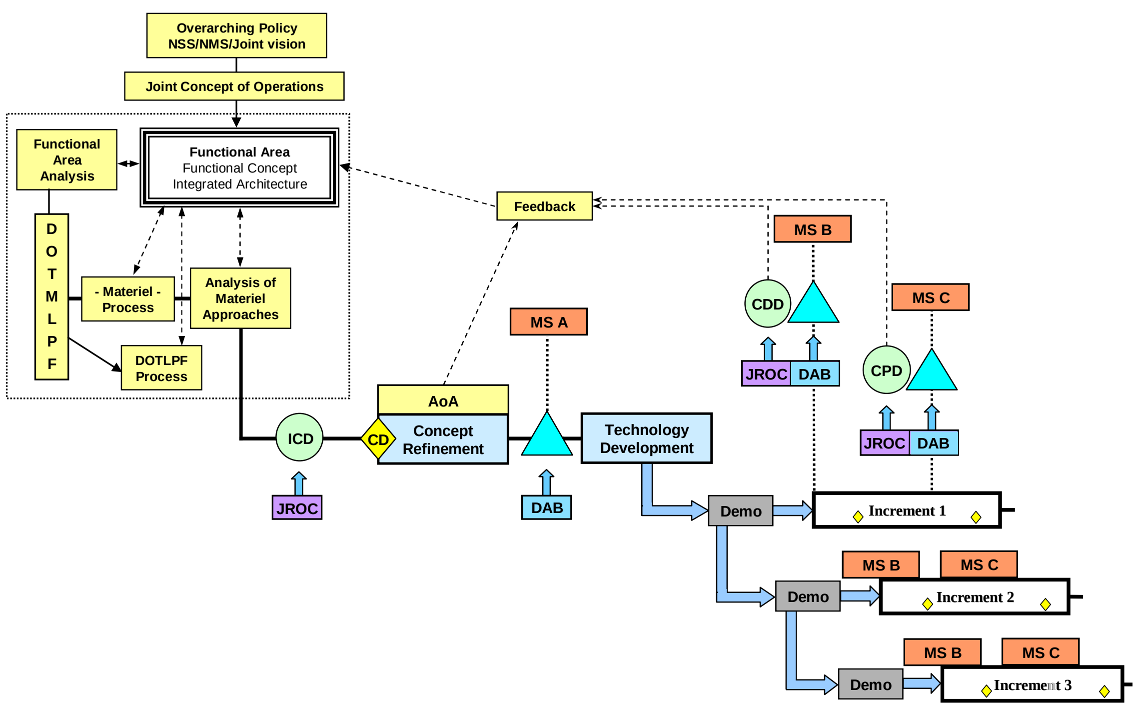


Figure 10 Requirements and Acquisition Process Depiction (From: Figure 2 in DoDI 5000.2, 2003)

[1] A detailed explanation of how the Systems Engineering Analysis Process can be customized to acquisition programs should be addressed in future work.

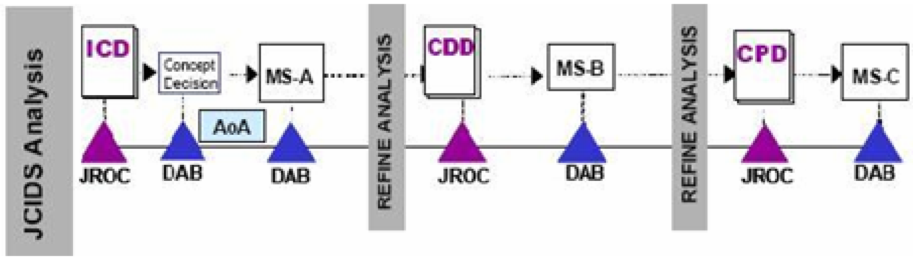
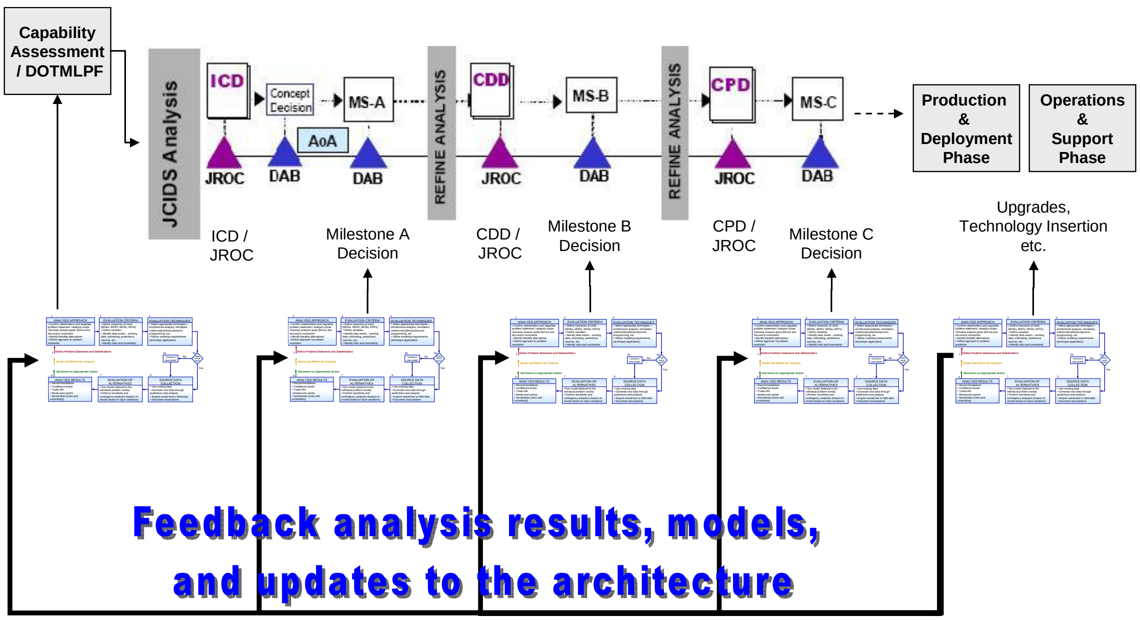


Figure 11 JCIDS Milestones



The process applies to and is iterated in every phase of the lifecycle. The analysis questions may vary in each phase based on the decisions that need to be supported.

Figure 12 Applicability of the Systems Engineering Analysis Process throughout the acquisition lifecycle.

E. CHAPTER SUMMARY

This chapter described how integrated architectures are used in the context of a systems engineering analysis process, and how that process may be applied to the JCIDS process and Defense Acquisition Process. The systems engineering analysis process and the architecture development process should be brought together into one process so that integrated architectures become the source data used to conduct systems engineering analyses, and in turn, the systems engineering analysis results and conclusions are applied directly to the improvement of these integrated architectures to deliver higher quality products to the warfighter.

Having now established that integrated architectures are useful data sets for informing various types of systems engineering analyses, and for informing the decision making processes described in Chapter II, the concepts of integrating and using architectures in a net-centric fashion is next addressed.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. ANALYSIS AND RECOMMENDATIONS FOR THE ARMY ARCHITECTURE INTEGRATION PROCESS

A. INTRODUCTION

This thesis chapter describes and analyzes key portions of the Army Architecture Integration Process (AAIP) in the context of the information presented in Chapters I through III, as well as additional research conducted on the concepts of architecture federation, architecture governance and net-centricity. Although the process that is analyzed in detail is Army-specific, the recommendations for the AAIP as it evolves are applicable in any program, component, mission area, or enterprise-level context. Section B provides an overview of the current version of the AAIP. Section C analyzes the objectives of the process. Section D analyzes the Integrated Architecture Development Process, the main process for implementing Army architecture integration. Section E provides a cursory analysis on two sub-process decompositions on the main process that have been included in the current version of the AAIP. Section F summarizes the concepts that have been recommended for use in extending the AAIP. Section G proposes a net-centric architecture integration environment using the information presented in the previous sections as design requirements. Section H summarizes the chapter.

Although this chapter details important aspects of significant concepts that enable architecture integration, it is not intended that this chapter be an all-encompassing treatment of the concepts presented. Rather, aspects of these concepts are highlighted in order to enable the AAIP and other like processes throughout the enterprise to be developed in more detail and to support conclusions regarding the premise of this thesis.

B. OVERVIEW OF THE ARMY ARCHITECTURE INTEGRATION PROCESS

The CIO/G-6 Army Architecture Integration Center (AAIC) is the Lead Integration Architect for the Army. The role of the AAIC is to govern architecture development across the Army and, amongst other responsibilities, certify that architectures are properly integrated where appropriate, meet the requirements detailed in the respective AV-1s and have use and utility for the customer. The AAIC is in the process of developing detailed instructions and guidance for use by the Army architecture community in conducting architecture integration and certification, as governed by the Lead Integration Architect. The purpose of the guidance is to establish a process that supports *Integrated Architecture Certification*, which is “a formal statement of adequacy provided by the Lead Integration Architect attesting that an integrated architecture facilitates and promotes traceability across Family of Systems (FoS) and System of Systems (SoS) architectures and is compatible among related architectures” (Army CIO/G-6 AAIC, 2007). The JCIDS and DoDAF definitions of *integrated architecture* presented in Chapter I of this thesis underpin the certification process and form the basis of the metrics required for measuring architecture integrity.

The Army Architecture Integration Process (AAIP) is being established in response to the large number of stovepiped architectures within the Army, and in an effort to transform Army architecture development and integration activities into a net-centric environment. The process is in its early development and stakeholder coordination stages, and once proved successful on architecture projects managed by the AAIC, it will be extended to the rest of the Army for implementation. Initial drafts of the AAIP describe its intent to develop a methodology for achieving Army Architecture Integration; to describe the format in which architecture data is to be delivered as well as the method of transfer to AAIC; and the criteria to be adhered to during architecture certification testing. Furthermore, the AAIP will define the roles and responsibilities of organizations within each of its sub-processes (Army CIO/G-6 AAIC, 2007).

1. AAIP Objectives

The AAIC specifies the following objectives for enabling the delivery of fully integrated Army architecture products in the AAIP v0.29:

- Ensure the formation of collaborative Integrated Product Teams (IPTs) as required to manage architecture integration for each project from the outset.
- Certify that the required architecture views adhere to JCIDS, DoDAF and Army directives.
- Certify that architectures use a common taxonomy for all architecture data.
- Ensure that the required architecture products are consistent and appropriately inter-related.
- Ensure architecture integration efforts are capabilities based and JCIDS compliant where necessary.
- Ensure that the required views are electronically generated from a cohesive database with a single robust integrated data model.
- Ensure data architectures are compliant with Core Architecture Data Model (CADM) and supporting architecture data standards.
- Ensure that interface descriptions depict the correct messages and data exchanges between domains.

As the AAIP evolves, these objectives will be decomposed and synthesized into a set of criteria against which architectures undergoing the certification process will be evaluated. This set of criteria will provide objective and quantitative metrics for measuring the integrity of architectures and reporting progress towards a goal of 100% integration.

2. AAIP Integrated Architecture Development Process

Figure 1 in Chapter I, shown again below as Figure 13, illustrates the Integrated Architecture Development Process proposed in (Army CIO/G-6 AAIC, 2007), which is an iterative, overall lifecycle process for the development of integrated architectures as viewed from the perspective of the Lead Integration Architect for the Army (AAIC). The process includes each organization's roles and associated responsibilities for accomplishing specific activities within the integrated architecture development process. A key function of this process diagram is to identify how the Army CIO/G6 AAIC manages, coordinates and facilitates product development and delivery, and thereby provides the organizations involved with the information necessary to recommend improvements and a more efficient process flow. The intended result is a coordinated AAIC- (and then Army-) wide process that supports DoD Enterprise Architecture policies and guidance presented in Chapter II, and incorporates recent U.S. Government Accountability Office (GAO) recommendations pertaining to DoD Business Enterprise Architecture (GAO-07-451, 2007).

The process steps are depicted in Figure 13, and are described in greater detail in Table 7.

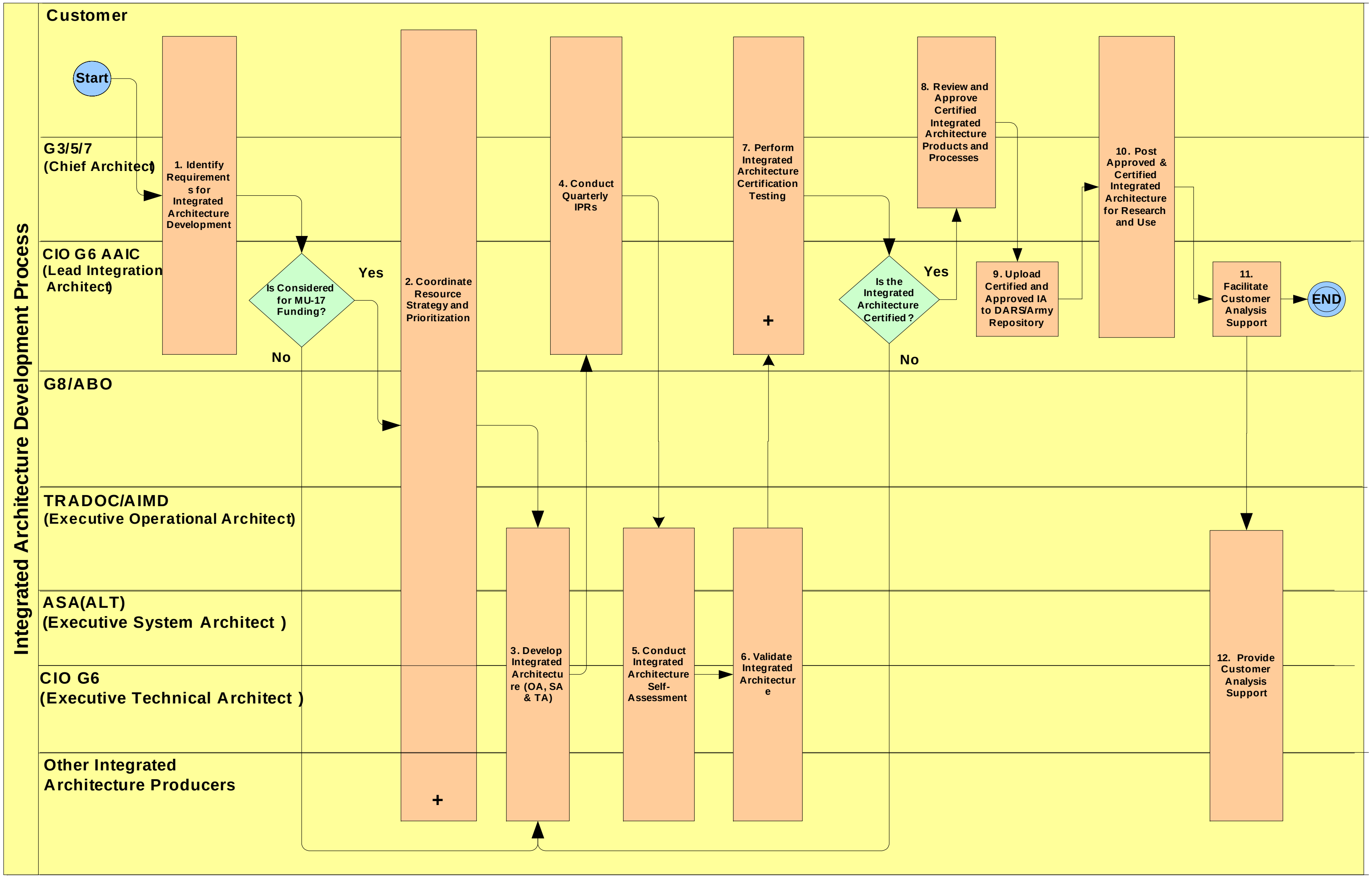


Figure 13 AAIP Integrated Architecture Development Process

Process Name	Process Description
1. Identify Requirements for Integrated Architecture Development	The Lead Integration Architect G-6/AAIC initiates a notification requesting the Customer and G/3/5/7 to identify requirements for developing a Capability based integrated architecture. Responsible authority for completion of this process: G6/AAIC Estimated time of completion: 30 Apr preceding FY.
2. Coordinate Resource Strategy and Prioritization	G6/AAIC directs the requirement for AV-1s integration, and requests Executive Architects and Other Architecture Producers to submit an AV-1 Summary, defining the purpose, scope, estimated cost, milestones, schedule, and associated deliverables. AV-1s are then prioritized and considered for MU-17 funding. G6/AAIC coordinates with the stakeholders to determine resource strategy and synchronize the integrated architecture requirements with set priorities. Following AV-1 approval of the overall Work Plan, Executive Architects and Other Architecture Producers are responsible for producing a full AV-1 for each funded project. Please see Sub Process 1 for further details. Responsible authority for completion of this process: G6/AAIC. Estimated time of completion: 01 Sep preceding FY.
3. Develop Integrated Architecture (OA, SA & TA)	Following receipt of AV-1 approval, Executive Architects and Other Architecture Producers develop required integrated architecture, underlying information/data using a Capability based methodology and process. The Executive Architects and Other Architecture Producers must reuse, where appropriate, relevant Certified and Approved integrated architecture and underlying information/data from previous projects in their product development. Responsible authority for completion of this process: Executive Architects and Other Architecture Producers. Estimated time of completion: Project Dependent.
4. Conduct Quarterly IPRs	G6/AAIC will conduct quarterly Interim Progress Review (IPRs) in coordination with G3/5/7 and Customer: Executive Architects and Other Architecture Producers will brief on architecture development status, coordination of processes and data across all projects in the Work Plan interim milestones, deliverables schedule, and risk assessment analysis to the Director of G6/AAIC. These IPRs will help G6/AAIC to mitigate risk assessment. Responsible authority for completion of this process: G6/AAIC. Estimated time of completion: Jan, Apr and Jul

Process Name	Process Description
5. Conduct Integrated Architecture Self-Assessment	After the Completion of the Integrated Architecture development, the Executive Architects and Other Architecture Producers assess their own architectures through the OMB recommended Assessment Tool. This assessment forms a vital part of the Army Quality Control (QC) process for the production of robust integrated architectures and a methodology to mature Army Processes. Responsible authority for completion of this process: Executive Architects and Other Architecture Producers. Estimated time of completion: Project Dependent
6. Validate Integrated Architecture	The Executive Architects and Other Architecture Producers will conduct an internal Architecture Validation Board (AVB) with the Subject Matter Experts (SMEs) to validate architectural content i.e. data/information (e.g., common naming conventions, definitions, relationships, and values). Responsible authority for completion of this process: Executive Architects and Other Architecture Producers. Estimated time of completion: Project Dependent
7. Perform Integrated Architecture Certification Testing	G6/AAIC in collaboration with G3/5/7 and the Customer will ensure that the Operational, System, and Technical Architecture information/data is consistent, integrated, trace one another and meet Customer requirements. The Integrated Architecture Certification Process focuses on the completeness of the architecture and on cross-boundary architecture integration (e.g., domains, mission areas) as well integration/consistency/traceability of architectural information/data outlined above. Responsible authority for completion of this process: G6/AAIC. Estimated time of completion: 30 days after receiving the Integrated Architecture from the Architects.
8. Review and Approve Certified Integrated Architecture Products and Processes	G3/5/7 and the Customer will review and approve the Certified Integrated Architectures in a periodic Council of Colonels (CoC) and Battle Command General Officer Steering Committee (BC GOSC). Responsible authority for completion of this process: G3/5/7. Estimated time of completion: 30 days Note: It is intended that Certification and Approval process will run concurrently.

Process Name	Process Description
9. Upload Certified and Approved IA to DARS/Army Repository /AKO	G6/AAIC will register Certified and Approved Integrated Architecture (including ALL underlying information/data) to the DoD Architecture Registry System (DARS) and make it available for other agencies' reuse. Responsible authority for completion of this process: G6/AAIC. Estimated time of completion: 2 weeks
10. Post Approved & Certified Integrated Architecture for Research & Use	G6/AAIC will disseminate Certified and Approved Integrated Architecture to the Customer community for Research and Use. Responsible authority for completion of this process: G6/ AAIC. Estimated time of completion: 2 Weeks (Concurrent with Activity 9)
11. Facilitate Customer Analysis Support	G6/AAIC facilitates/coordinates with the Executive Architects and Other Architecture Producers to provide Customer Analysis Support. Responsible authority for completion of this process: G6/AAIC Estimated Time for Completion: From the publishing of the Certified and Approved Architectures in DARS. (Concurrent with Activity 11)
12. Provide Customer Analysis Support	Executive Architects and Other Architecture Producers will provide analysis support to the Customer as required. Responsible authority for completion of this process: Executive Architects and Other Architecture Producers Estimated Time for Completion: Project dependent.

Table 7 Integrated Architecture Development Process Descriptions (From: Annex A, Army CIO/G-6 AAIC, 2007)

3. AAIP Integrated Architecture Development Sub-Processes

Two sub-processes have been defined in version 0.29 of the AAIP: the Coordinate Resource Strategy and Prioritization (a decomposition of Main Process Activity 2) and the Integrated Architecture Certification Process (a decomposition of Main Process Activity 7). The Coordinate Resource Strategy and Prioritization process depicts a Work Plan Prioritization process that iterates every FY, and details G6 AAIC coordination with G3/5/7 and Executive Architects in prioritizing Customer requirements for the development of integrated architectures and resource allocation. The Integrated Architecture Certification Process depicts a process for certifying that architecture data is integrated, and ensuring that the architecture data are consistent with the resultant architecture products (i.e., there are common points of reference linking operational and systems data, as well as linking systems data and technical data).

Detailed analysis of these two activities are beyond the scope of the thesis, although the Prioritization sub-process is briefly analyzed towards the end of this chapter for its applicability to the systems engineering analysis process presented in Chapter III.

C. ANALYSIS OF THE AAIP OBJECTIVES

This section analyzes the AAIP objectives presented in the previous section in the context of the integrated architecture criteria found in policy and guidance.

In Chapter II, DoDAF guidelines for the development and integration of architectures and characteristics of integrated architectures were summarized. These “features of integrated architectures” may be used in the development of essential elements of analysis (EEAs) and top-level criteria (Measures of Effectiveness) as the AAIP’s objectives are refined. These top-level criteria can be further decomposed into quantifiable metrics (Measures of Performance) for use in evaluating architectures for conformance with DoDAF guidelines and integrity. Thus, the AAIC can apply the systems engineering analysis process presented in Chapter III to conduct its own mission[2].

A brief example of how AAIC can use the systems engineering analysis process to conduct its mission is provided herein. The guidelines for the development and integration of architectures and characteristics of integrated architectures presented in Chapter II have been rephrased into some notional EEAs and MOEs shown in Table 8. Some notional MOPs are also provided as an example of what is possible. The example MOPs assume (and require) that

[2] A full description of how the systems engineering analysis process is applied to the AAIC mission is identified as future work.

processes have been put in place for collecting these metrics. Table 8 addresses not only integrated architecture certification metrics, but also includes other architecture quality metrics. A comparison against the AAIP objectives shows that the AAIP objectives are currently focused entirely on the EEA “Is the architecture interoperable across the DoD?” This thesis recommends that a broader Architecture Quality Certification also be conducted that encompasses at a minimum all of the metrics outlined below, which are directly traceable to requirements in the DoDAF. An integrated architecture is, after all, limited in its utility unless it contains the data necessary for analysis, has “a purpose in mind,” is “simple and straightforward,” is “understandable among architecture users,” and “agile.” Architecture agility is the metric that is the focus of the thesis premise that integrated architectures have increased usefulness to the users of the systems they describe when they *can be interactively and dynamically updated and used in conjunction with systems engineering analyses to enable systems optimization*. The concept of architecture agility is discussed in more detail in the following sections of this chapter.

Essential Element of Analysis	Sample Measures of Merit	DoDAF Reference
Does the architecture have a purpose in mind?	**MOE 1**: The architecture's AV-1 articulates a specific purpose. **MOE 2**: The architecture's AV-1 provides evidence that the purpose is clearly understood by the stakeholders. **MOE 3**: The scope described in the AV-1 is traceable and appropriate to the purpose. **MOE 4**: The purpose aligns with the priorities of the community. **MOE 5**: The purpose contributes to the success of mission goals and objectives.	Volume I, Para. 2.1.1
Is the architecture simple and straightforward?	**MOE 6**: The architecture effort is adequately focused to obtain an acceptable return on investment. **MOE 7**: The level of detail in the architecture is appropriate for achieving the desired objectives.	Volume I, Para. 2.1.2
Is the architecture understandable among its users?	**MOE 8**: User feedback indicates issues with comprehension of the information in the architecture are being addressed. **MOP 8.1**: Number of help requests (tracked over time, should be decreasing) **MOE 9**: Issues with understanding the information in the architecture are able to be resolved quickly. **MOP 9.1**: Time elapsed between question and answer (hrs / days) **MOE 10**: Architectures provide a clear representation of the information by using common terms and definitions and avoiding extraneous information. **MOP 10.1**: Percent (%) breakout of user satisfaction (scale of 1 to 5)	Volume I, Para. 2.1.3

Essential Element of Analysis	Sample Measures of Merit	DoDAF Reference
Is the architecture interoperable across the DoD?	**MOE 11**: The architecture is consistent with DoD policy and guidance. **MOE 12**: The architecture contains a mapping or standardization of terms, definitions, and relationships across the architecture that are linked via underlying data relationships. **MOP 12.1**: Percent of activities defined in the activity models (OV-5) that are the same as those that are associated with operational nodes in an Operational Information Exchange Matrix (OV-3) (Objective: 100%) **MOP 12.2**: Percent of organizational entities identified in Operational Node Connectivity Descriptions (OV-2) that are the same as the organizational entities identified in a Command Relationship Hierarchy (OV-4) (Objective: 100%) **MOP 12.3**: Percent of systems represented in the Systems Interface Description (SV-1) that are the same as the systems identified in the Systems Communication Description (SV-2) (Objective: 100%) **MOP 12.4**: Percent of standards identified in the Technical Standards Profile (TV-1) that are the same as those identified in the Systems Interface Description (SV-1) (Objective: 100%) **MOE 13**: Architecture descriptions clearly describe external interfaces with Joint, multinational, and commercial components, using a method that is consistent with that used to describe internal relationships. **MOE 14**: Architecture descriptions are readily available across the Enterprise for decision process analyses, reuse in other architecture efforts, and mission support. **MOE 15**: Users are applying and reusing data in other architectural efforts.	Volume I, Para. 1.2.2; Volume I, Para. 2.1.4; Volume I, Para. 2.4.2
Is the architecture agile?	**MOE 16**: The architecture is modular, reusable, and decomposable to achieve agility **MOE 17**: Architecture descriptions consist of related pieces that can be recombined with a minimal amount of tailoring to enable use for multiple purposes **MOE 18**: The architecture provides the means for functioning in a dynamic environment	Volume I, Para. 2.1.1

Table 8 EEAs, MOEs and MOPs for Evaluation of Architecture Quality

D. ANALYSIS OF THE AAIP INTEGRATED ARCHITECTURE DEVELOPMENT PROCESS

The Integrated Architecture Development Process demonstrates a well laid out swim lane process flow diagram, showing the roles of and interactions among the stakeholders, and in the accompanying annex (Table 7) it briefly describes each step, assigns responsibilities, and provides timelines for completion. The process is iterated once every fiscal year.

The main products that are intended to result from the Integrated Architecture Development Process are certified integrated architectures. Once these integrated architectures are successfully produced and certified, then what is done with them? Are they analyzed? Corrected? Improved? Used as entrance criteria – as evidence of good work – only to be put on the high shelf after the milestone review? The answer to what becomes of the architectures is not addressed in the current version of the AAIP. The Integrated Architecture Development Process excludes (deliberately or not) reference to any steps for maintaining the integrated architectures that are produced, once they reach the "end" of the process illustrated in Figure 13 As demonstrated in Chapter II, numerous policies and guides (e.g., JCIDS) reference the continual development of integrated architectures throughout the lifecycles of the systems it describes. As demonstrated in Chapter III, the iterative nature of analysis conducted on integrated architectures calls for the ability make changes and improvements to these architectures. Hence, there should be an extension or annex to the AAIP that describes how this architecture improvement can effectively be accomplished.

It is worth noting that a previous GAO report on the maturity of enterprise architecture programs (GAO-06-831, 2006) showed that the Department of the Army had not satisfied 55 percent of the core elements in GAO's Enterprise Architecture Management Maturity Framework (an element in Table 1 in Chapter II), which is a five-stage model for effectively managing architecture governance, content, use, and measurement. The Army's 55 percent overall dissatisfaction score is in comparison to those of the Air Force and Navy, which each had a much lower overall dissatisfaction score of 30 percent. Moreover, the Army had only fully satisfied 1 of the 31 core elements, in comparison with the Air Force, which fully satisfied 14 out of 31, and the Navy, which fully satisfied 10 out of 31 (GAO-07-451, 2007). Although these figures do not indicate exceptional performance by any of the three departments, these statistics indicate a large gap in maturity of Enterprise Architecture management between the Army and the other services.

As can be seen in Figure 14, the Army is a Component Layer member of the DoD's BMA Federated Architecture. With a successful development and implementation of the AAIP, accompanied by mechanisms for improving and optimizing the integrated architectures it produces, the Army has an opportunity to significantly improve its current score in Enterprise Architecture management maturity.

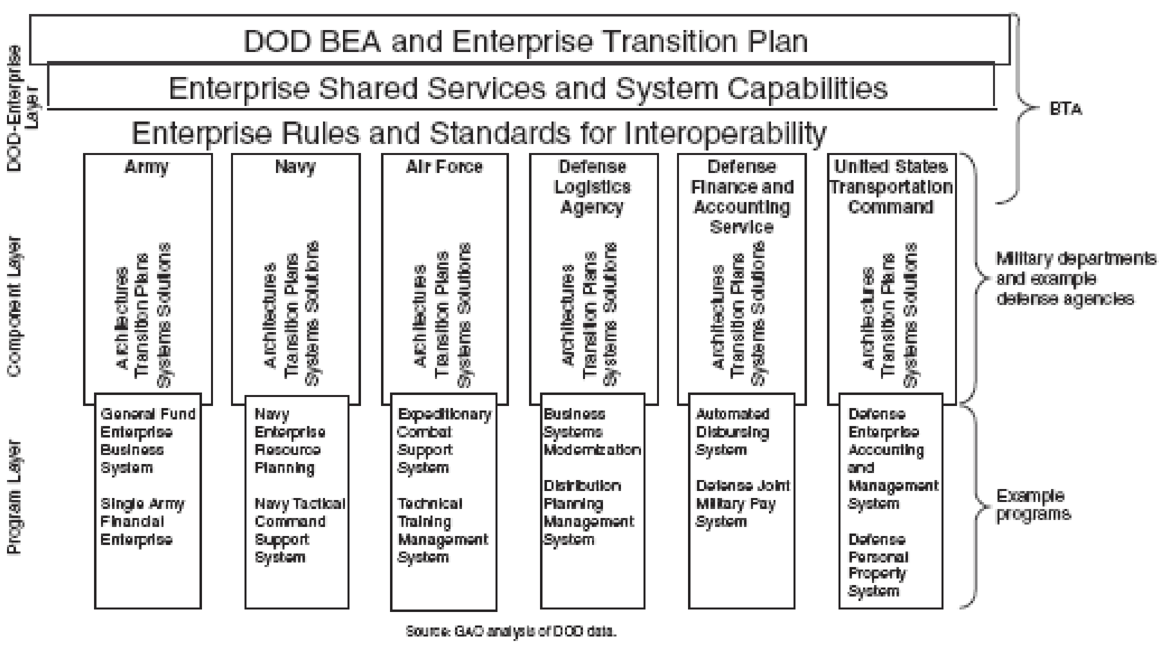


Figure 14 Simplified Diagram of DoD's Business Mission Area Federated Architecture (From: GAO-07-451, 2007)

As touched on in Chapter III, the mechanisms that need to be in place at the DoD- or even just the Army- level to enable improvement and optimization of integrated architectures involves no trivial effort. It is an accomplishment indeed even just to successfully achieve the production of a baseline integrated architecture that meets the requirements in DoDAF, is data based, and is detailed enough for use in a one-time analysis; let alone to have mechanisms in place for efficiently providing and inserting feedback, lessons learned, and improvements back into that integrated architecture as it evolves. Yet the premise of this thesis demands more than the successful production of an integrated architecture. The integrated architecture must be agile and dynamically updateable to reach its maximum potential utility.

The research on mechanisms that enable efficient improvement and optimization of integrated architectures resulted in a detailed exploration of three enabling concepts: architecture federation, architecture governance, and net-centricity. An overview of each concept is provided in the following sections, along with suggestions for implementation in the AAIP based on a study of the literature.

1. Analysis of Architecture Federation Concept

As previously discussed, integration of architectures involves establishing consistent architecture data elements through multiple views. Federation of architectures is a separate but related concept, which involves linking disparate architectures across the enterprise, providing a “holistic enterprise view” that enables cross-program, cross-component and cross-mission area assessment of interoperability, gaps, and reusability; supporting decision making at each level. A *federated architecture* is a distributed strategic information asset base that “provides a framework for enterprise architecture development, maintenance, and use that aligns, locates, and links disparate architectures and architecture information via information exchange standards to deliver a seamless outward appearance to users.” Thus, federation of architectures allows autonomy and local governance of architectures, while at the same time enabling the rest of the enterprise to benefit from their content so that issues that cross multiple areas can be addressed. The DoD has chosen to apply this approach to the GIG architecture in order to support construction of a more robust environment for understanding the enterprise (Volume I, Section 1.2.2 and Section 2.4.1, DoDAF, 2007). The Director, Architecture & Interoperability OSD(NII) Deputy CIO recently published the GIG Architecture Federation Strategy, which outlines how existing architectures will be linked and related to provide a comprehensive view of the DoD enterprise, while allowing for autonomy of individual architectures (OSD(NII) DCIO, 2007).

Both integrated and federated architectures are necessary in the development of a net-centric environment (discussed later in this chapter) and in the sharing of information. “As the DoD becomes increasingly networked, integrated and/or federated architectures become essential in organizing the vast array of information and complex relationships” (Volume I, Section 2.4.1, DoDAF, 2007). Presently, DARS implements a set of federation standards that catalogs and links architecture content from any repository that supports those standards. (Volume III, Section 2.7, DoDAF, 2007).

“In order to federate architectures, there must be elements of semantic agreement” across the architectures so that the user have a common language to facilitate consistency and integration (Volume I, Section 2.4.3, DoDAF, 2007). Semantic agreement can be achieved via the following practices:

- *Adherence to a common framework (e.g., DoDAF)*; which includes the use of common data element definitions, semantics, and data structures for all architecture description entities or objects; to ensure standard representation of architecture regardless of mission or capability area
- Conformance to common or shared architecture standards, which increases interoperability
- *Use of enterprise taxonomies and authoritative reference data*, which set the context for aligning mission area activities and organizing component architectures.

Establishing *authoritative reference data* is an important aspect of architecture data quality, which in turn affects the ability to analyze architectures and compare/integrate independently developed architectures. *Reference data* is the term used to refer to "acceptable or allowable data instance values," and an *authoritative reference data* set refers to "a set of element values that are approved or designated for use" by recognized authorities, or *authoritative sources* (Volume III, Section 2.6, DoDAF, 2007). For example, the Joint Staff is identified as the authoritative source for the Universal Joint Task List (UJTL), which is an authoritative reference data set used in operational architectures (Volume III, Section 2.8, DoDAF, 2007).

The DoDAF encourages conducting information gathering, analysis, and synthesis into an integrated architecture using "an integrated tool or a set of tools," for consistency and version control. It provides criteria for the selected tools, including capability to produce consistent products/views by performing cross-product checking, capability to store, update, and retrieve architecture data and their relationships, capability to automatically generate an integrated dictionary, and capability to import/export to/from a CADM conformant database (Volume II Section 2.3.1, DoDAF, 2007). However, there are some challenges related to institutionalizing architecture into DoD core processes. The current practice of developing architectures by many organizations within DoD independently of one another and often using different tools raises several concerns. Architects and architecture end users require the capability to perform global horizontal and vertical searches for architecture data required for analysis or other architecture development efforts. A consistent set of standards for architecture configuration management is also needed for determining development status, quality, and authority of data. Furthermore, a standard methodology is needed for specifying linkages between architectures developed using different tools in independent repositories (OSD(NII) on GIG Federated Architecture Strategy, 2007).

Architecture federation is intended to address these issues. There are many benefits of federation for decision makers, architects and architectural governance bodies that are articulated in the GIG Federation Strategy. These benefits are summarized below (Section 6, GIG Federation Strategy, 2007).

Federation benefits DoD decision makers by:

- Enabling rapid access to information for strategic decisions
- Improving information sharing of architecture content
- Providing understanding of interactions and interdependencies
- Supporting portfolio management of technology options
- Supporting the Joint Warfighting Capability of the DoD
- Reducing cost of Defense Operations

Federation benefits DoD Architects by:

- Promoting distributed configuration management
- Providing clear “stopping” rules for Enterprise Architecture development
- Increasing agility

Finally, federation benefits architectural governance bodies by:

- Setting enterprise boundaries
- Promoting autonomy or distributed governance

It is interesting to note that increased agility is specifically called out as a benefit of architecture federation, since it is the premise of this thesis that architectures are most useful to their users when they can be quickly updated and analyzed. The author argues that this benefit, although called out in the GIG Federation Strategy as a benefit to DoD Architects, also benefits DoD decision makers and warfighters since the decisions often need to be made quickly. Architecture agility reduces the turn around time on analyses by reducing the time needed to conduct what-if drills and alternate scenario excursions. ”Users can search the GIG Architecture registry and find existing architecture content, significantly reducing the time and cost for new architecture development, fielding of a new capability, and gaining improved interoperability “out of the box.” By using these building blocks, warfighters can swiftly adjust their architectures to meet changing business and mission needs" (Section 6, GIG Federation Strategy, 2007).

To summarize the value of architecture federation, integrated architecture efforts, particularly Joint architectures, have architects, subject matter experts, analysts and other developers and users of architecture data from many different organizations using many different tools and repositories. The intent of the architecture federation concept is to make the data in these disparate tools accessible and usable by all.[3]

2. Recommendations

Having common reference data is a theme that runs through all three concepts presented in this chapter (architecture federation, architecture governance and net-centricity). In federated architectures, having common reference data not only enables local governance, but enables control and dissemination of standardized terms and definitions by the appropriate authorities. Each member of the federation maintains the data pertaining to their area of expertise. This data is then made available to all members of the federation for use in architecture development and/or analysis.

It is recommended that Army other DoD architects collaborate to develop authoritative reference data in preparation for implementation of the federation strategy. The following approach, initially described in (Giammarco et. al, 2005), is presented as an initial baseline for refinement by the community.

<u>Define Reference Lists.</u> Operational, systems and technical subject matter experts determine and define appropriate reference lists, which are pick lists from which to choose "acceptable or allowable data instance values." Some example reference lists are Battle Phases, Force Structure Elements, Army

[3] Further exploration of the specific challenges associated with sharing data between tools is a good topic for another thesis, and is proposed in Chapter V as future work.

Universal Task List (AUTL), Universal Joint Task List (UJTL), "Reports, Messages, ISR & Telemetry" List (ReMIT) List, Format Parameters, Systems, Network Services, Networks and Technical Standards.

Define Reference Matrices. Operational, systems and technical subject matter experts determine and define appropriate *reference matrices*, which show relationships and dependencies among the data instance values. A reference matrix may be set up on a spreadsheet by listing data instance values from one reference list down the first column and data instance values from another reference list across the first row. The cells of the matrix are then populated to show the relationship between data instance values from the two lists. Some example reference matrices (along with somewhat dated but nonetheless useful example data instance values) are described in Table 9.

Reference List Name	**Reference List Description**
Operational Tasks performed during *Battle Phases*	This matrix captures the operational tasks (i.e. AUTLs and/or UJTLs) that are performed during each phase of battle (from Objective Force: Unit of Employment Concept, 7 Aug 02): Entry, Shape, Decisive, and Transition (e.g., Conduct Landing Zone Operations during Entry phase).
Force Structure Elements performing *Operational Tasks*	This matrix captures each operational task performed by each force structure element according to the doctrinal requirements of the unit being analyzed (e.g., 3ID/UE-x/DIV HQ/DTAC CP1/ADA performs Conduct Landing Zone Operations).
ReMITs required to execute *Operational Tasks*	This matrix captures all C4ISR information (Reports, Messages, ISR, and Telemetry), known in short as ReMITs, needed for or generated by the completion of each operational task. Some tasks call for ReMITs being generated (produced) as output of the task, and some tasks call for ReMITs being required (consumed) as input to the task. This matrix just captures the doctrinal association of the ReMITs with each task, not who specifically is producing and consuming the information (e.g., an INTSUM (Intelligence Summary) is required to execute Conduct Landing Zone Operations).
ReMITs exchanged by *Force Structure*	This matrix captures each ReMIT produced and consumed by each force structure element. This defines a general flow of information that is based on the unit's standing operating procedures (SOP) (i.e. "business practices") that is

Reference List Name	Reference List Description
Elements	independent of mission or scenario. This matrix provides information on C4ISR production and consumption at each element in the unit. This matrix is automatically cross-referenced with both the "Force Structure Elements performing Operational Tasks" and the "ReMITs required to execute Operational Tasks" doctrinal matrices to ensure the ReMIT flows defined in this SOP matrix support the operational tasks performed by each element in the unit. If any inconsistencies are found, the matrices are revisited and the necessary corrections are made before using the data in subsequent analyses.
Format Parameters associated with each *ReMIT*	Each ReMIT may occur in one or more formats: data, imagery, voice or vidstream. Every potential format of each ReMIT has a set of parameters assigned to it: frequency of occurrence (per hour) for each battle phase, security classification, precedence, criticality and perishability. In addition, size (in Kilobytes, before system and network overhead) is populated for the non-streaming formats of data and imagery; and duration (in seconds) and data rate (in kbps) are populated for the streaming formats of voice and vidstream. These format parameters quantify each ReMIT to support network loading calculations.
Systems resourced to *Force Structure Elements*	This matrix shows the names and quantities of systems in the System Architecture (SA) that are assigned to each element in the force structure. Examples of systems include the Army Battle Command System (ABCS) applications and their application servers, Voice over Internet Protocol (VoIP) phones, generic computers/laptops and collaboration/VTC equipment.
Operational Tasks supported by *Systems*	This matrix is used to help narrow the assignment of a system for an information exchange. It includes all the operational tasks that a particular system would be used to support. This information is provided by individual system subject matter experts.
ReMITs exchanged by *Systems*	This matrix is used to assign systems to an information exchange. It ensures that an information exchange is assigned to systems that are capable of exchanging it.
Network Services available to *Systems*	This is a set of mappings that are combined with programming logic to determine the network service used in the sending and the receiving of a ReMIT. Example network services include VoIP, Collaboration, Tactical Web (TACWEB), Email, and Peer-to-Peer. A different set of network services can be defined based on the given system architecture.
Networks	The assignment of network is made based on the system

Reference List Name	Reference List Description
available to *Systems*	architecture source data and some programmed logic. Network examples are Unclassified but Sensitive Internet Protocol Router Network (NIPRNET), Secret Internet Protocol Router Network (SIPRNET), Joint Worldwide Intelligence Communications System (JWICS) and Combat Service Support (CSS).
Technical Standards supported by *Systems*	This matrix captures the technical standards associated with systems in a given architecture. Some examples include ITU-T H.261 Video CODEC for Audiovisual Services at p x 64 Kbps, March 1993, and JPEG File Interchange Format, Version 1.02, September 1992.

Table 9 Example Reference Matrices (From: Giammarco et al., 2005)

Customize / Optimize Reference Matrices. Using the reference lists and reference matrices; architects, analysts, and other users can perform their respective tailoring and optimization of the data instance values and their relationships. This step entails full collaboration among OA, SA and TA architects working on a given architecture to generate the integrated architecture in parallel with the analysis process described in Chapter III.

Develop Rule Sets / Use Cases. Architects construct sequences of events and rules involving the cause/effect relationships (e.g., OV-6a,b and SV-10a,b) that trigger operational, system and technical threads required to conduct missions. Developing these rule sets are more important (and more difficult) than developing the actual threads (i.e., OV-6c and SV-10c), because the latter only represent one possible instance of the many possible implementations captured by the rule sets. Doing so, however, results in a more robust model and enables simulation and emulation to find optimal solutions under different scenarios and circumstances[4]. These products draw on the reference lists and reference matrices, significantly reducing the workload and freeing up time and resources of the architects to develop the rule sets.

Generate Architecture Instance. Through the above process, conducted in parallel with the systems engineering analysis process, an optimal

[4] An elaboration on the need for the a and b views of the OV-6 and SV-10 products is reserved for a future paper.

configuration for a given architecture can be reached. After the analysis is complete, a version-controlled architecture "instance" can be delivered with all necessary architecture products containing the appropriate information required for each view, thus resulting in an appropriate integrated architecture with corresponding analysis to support a milestone decision point.

Having authoritative reference lists and matrices, and having these federated, will support a significant reduction in the "Source Data Collection" step of the systems engineering analysis process presented in Chapter III. This reference data will also significantly reduce the effort required to update architectures based on these lists, in that changes to the reference data can be automatically reflected in the working architecture. As such, quick turn studies can be performed *while the architecture is still under development*, and therefore result in a *better integrated architecture*.

The mappings in some of the matrices in Table 9 are (or should be) standard within every architecture, per doctrine, whereas some will be dynamic and dependent on the assets and capabilities of the specific architecture under development. The fundamental concept is to maximize the amount of information that can be standardized and reused across all architectures, and provide a baseline for customization for those mappings that need to be optimized for a specific architecture, as well as a data set on which to draw when developing the rule sets for the threaded products. The matrices are the source for capturing relationships among technical, systems, and operational data, so that resulting OVs, SVs, and TVs are completely consistent and integrated with one another. Furthermore, the matrices allow relationships among all reference data to be determined in a consolidated manner (consistent with the "Only Handle Information Once (OHIO)" net-centric principle that is noted in Section 3 below), and are the key to producing completely consistent architecture views. Moreover, the matrices are modular, such that approved architectural updates to the reference data can be propagated through all dependent federated architectures at once.

The DoDAF describes the consistent manner in which to facilitate the use of integrated and federated architectures at any tier in the DoD organization. This advice consists of 1) Use the DoDAF for its standard terms, definitions, data elements, and their relationships; 2) Use the CADM for its canonical data model that identifies data attributes and relationships; and 3) Use the DARS for net-centric use and management of the data (Volume I, Section 3.3, DoDAF, 2007). The use of DARS is further discussed in the section on Net-Centricity.

The general recommendation is to further explore the above process for developing reference data in a manner that allows maximum reuse across the DoD enterprise, consistent with the GIG Federation Strategy. With respect to the AAIP, it is recommended that this process be reviewed, improved, and considered for adoption into the decomposition of Activity 3, Develop Integrated Architecture (OA, SA, TA), in the AAIP Integrated Architecture Development Process (Figure 13). It is also recommended that the Army Executive Architects federate their databases using the DoDAF, the CADM and the DARS as described above.

3. Analysis of the Architecture Governance Concept

Recall from Chapter II that *governance* is defined as “the processes and systems by which an organization and system operates, the rules of engagement, the escalation mechanisms, the change management and conflict resolution mechanisms, and the enforcement mechanisms.” In April 2007, the GAO published its report on “BUSINESS SYSTEMS MODERNIZATION: Strategy for Evolving DOD's Business Enterprise Architecture Offers a Conceptual Approach, but Execution Details Are Needed” (GAO-07-451, 2007). The GAO recommends in their report that the DoD address the question of how architecture federation will be governed, placing special emphasis on the need for defining and assigning roles and responsibilities. The DoDAF also calls out the need for a governance structure for providing direction and oversight over federated architectures. Such a structure ensures that architectures are developed and used under appropriate authority and direction and with the correct guidance, and enables architecture monitoring to assert affirmative or remedial actions when necessary (Volume I, Section 4.1, DoDAF, 2007). Both the DoDAF and the Business Mission Area (BMA) federation strategy (GAO-07-451, 2007) discuss a concept for a governance framework called *tiered accountability.* Through tiered accountability, “authority and responsibility of elements of the enterprise architecture are distributed throughout the organization,” and architecture owners are responsible for governing their own architecture holdings. Under tiered accountability, architecture owners are responsible for ensuring their products “meet their specific purpose, are in accordance with policies and directives from the tiers above, and allow for federation with disparate architectures“ (Volume I, Section 4.1, DoDAF, 2007). The enterprise, component and program levels depicted in Figure 14 are the tiers for the DoD. Each of these tiers has its own unique goals for their architectures, but also has responsibilities to the tiers above and below it. Each tier must be autonomous, but also support linkages and alignment from the program level through the component level to enterprise level (GAO-07-451, 2007).

There is a connection between governance over an architecture and the integrity of the architecture data. The DoDAF states that “roles and responsibilities should be in place to account for the development of architectures, ensure alignment between tiers, and maintain architecture data integrity” (Volume I, Section 4.1, DoDAF, 2007). A rigorous framework for architecture governance supports the efficient improvement and optimization of architecture because this underlying structure facilitates coordination among the constituent organizations, which increases the reliability, completeness and consistency of the data in the architecture – a major prerequisite to analysis as described in Chapter III.

4. Architecture Governance Issues

A primary issue that GAO has with the BMA strategy is that roles and responsibilities of the respective members of the federation are not clearly defined. ASD(NII)/CIO officials have responded that this and other governance functions critical to the successful execution of the BMA are defined at the mission area level, to include defining roles and responsibilities of its member components and programs. Figure 15 shows that "mission areas" are decomposed into "domains," and that governance functions are assigned to organizational entities for each "mission area." For example, the Defense Business Systems Management Committee (DBSMC) is responsible for governance of the BMA, which consists of the following "domains":

- Weapons System Lifecycle Management
- Material Supply and Service Management
- Real Property & Installation Lifecycle Management
- Human Resources Management
- Financial Management

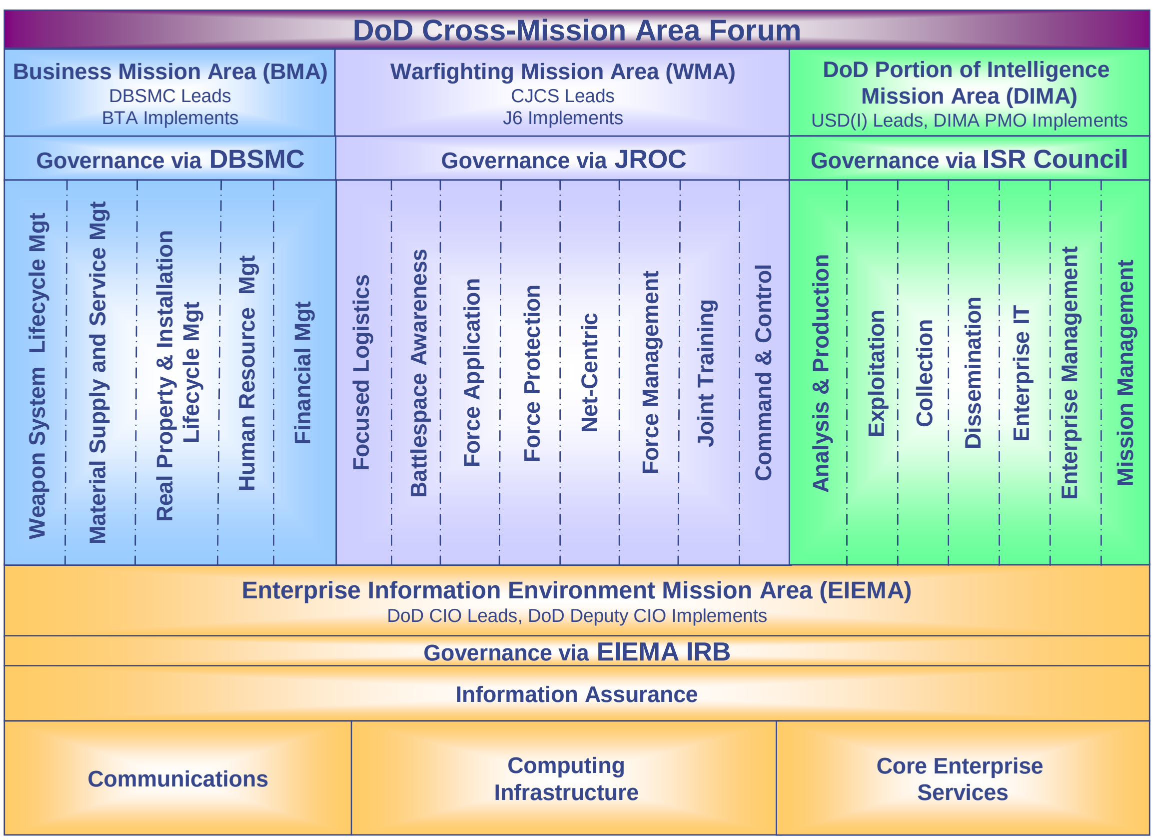


Figure 15 Mission Areas and Their Domains (From: IT PfM Team, 2007)

From examining the domains, it is clear that they are not themselves "components," rather they are functions that are executed by components (e.g., military departments). The DBSMC is therefore the coordinating body that oversees execution of these functional domains across the components. GAO's issue is that DoD has not coordinated specifically who, among the components (organizational entities), is responsible for ensuring that their respective architectures align to the BEA; ensuring that their priorities fit with overall enterprise priorities; providing, overseeing, funding and staffing needed training on the concepts of the BMA federation strategy; and providing metrics for use in gauging progress towards implementation of the BMA federation strategy concepts (GAO-07-451, 2007). The GIG Federation Strategy, published four months after this GAO report, defines general roles and responsibilities at the Enterprise, Department, Mission Area, Component and Program levels (GIG Federation Strategy, 2007).

5. Recommendations

The Army has already begun to address the GAO requirement for defining roles and responsibilities, at least for Architecture Development and Integration overseen by the CIO/G-6 AAIC, as evidenced in the Architecture Development and Integration Process (see Table 7). The following recommendations pertaining to architecture governance are provided for consideration by the Army as well as other elements in the DoD Enterprise.

a. Federation Strategy Training

OSD(NII) DCIO has planned to host a series of three workshops in September and October 2007, whose purpose is to gather requirements from agency and service component stakeholders on their needs for formal architecture education (Damashek, 2007). In the context of the issues summarized above, this activity could be applied toward an answer to GAO's recommendation to delineate who is responsible for providing, overseeing, funding and staffing training on the concepts of the BMA federation strategy. The author of this thesis is a participant in this workshop series, and has suggested that training on the BMA and GIG federated architecture strategies be included as a requirement for the architecture education curriculum.

b. Milestones and Measures

The GAO recommends in their report that the DoD address the question of what milestones will be used to measure progress and results towards implementation of the BMA federated architecture strategy. In order to fulfill this recommendation, the DoD can develop a set of measures such as those exemplified in Table 8, except customized for the high-level activities, capabilities, products, and services intended to facilitate implementation of federation strategy concepts.

c. System of Systems Engineering

Recall the discussion in Chapter III on System of Systems Engineering (SoSE). SoSE emphasizes "discovering, developing, and implementing standards that promote interoperability among systems developed via different sponsorship, management, and primary acquisition processes" (p. 53, Guide to SoSE, 2006). The successful application of SoSE across the many constituent systems within the DoD enterprise would help to address GAO's governance concern. All organizations within DoD (including component and program owners of constituent systems) as well as those that interface with DoD (e.g., other federal agencies and multinational agencies) must collaborate to develop a successful SoS. Systems engineering, SoSE, and the systems engineering analysis process are tools whose value should be summarized and made available to these stakeholders in a coordinated, policy-driven way.

d. Authoritative Reference Data

In the previous section on architecture federation, the concept of subject matter experts maintaining and providing authoritative reference data was introduced, and referred to as a common theme that runs through the three concepts explored in this chapter: architecture federation, architecture governance and net-centricity. With respect to architecture governance, each organization in the DoD, at each tier of accountability, should be assigned the roles and responsibilities required for maintaining the reference data for which they are the subject matter experts, and that is needed by other organizations for constructing an integrated architecture. Roles and responsibilities may be delineated for both reference lists and reference matrices described in the previous section. For example, as mentioned earlier, the Joint Staff is identified as the authoritative source for the UJTL elements (Volume III, Section 2.8, DoDAF, 2007). With respect to the AAIP, it is recommended that publication and maintenance of pertinent reference data be defined and delegated to the appropriate authoritative sources.

e. DoDAF-Compliant Integrated Governance Architecture

Establishing a Governance Architecture, as discussed in Chapter II, is one of the four pragmatic challenges for the effective synthesis and deployment of SoS. Note the distinction between *Governance Architecture;* which is an *entity* that comprises "institutions, structures of authority and collaboration to allocate resources and coordinate or control activity" (p. 5, Guide to SoSE, 2006); and Architecture Governance, which is the *act* of governing architecture. What is being recommended as a result of the analysis above is that a "governance architecture" be created and represented using DoDAF with the same rigor with which one would create any other integrated architecture. That is, a governance architecture is and should be an integrated architecture in its own right, and should have an AV-1, AV-2, and corresponding OVs, SVs, and TVs that describe the interactions among its constituent decision makers, other enterprise-level users, components, programs, and business systems they use to effect governance.

The GIG Federation Strategy highlights that a key challenge related to institutionalizing DoD architecture into core processes is that "there is no comprehensive architectural description of the DoD Enterprise and its relationship between and among the entities that make up the enterprise that can be used to support department-level decision making." A governance architecture as described above would very precisely define the big-picture goal of DoD Enterprise Architecture in its OV-1, activity flows among organizations that need to collaborate in its OV-5, people or roles that need to communicate in its OV-2, what those people or roles need to communicate about in order to govern architectures in its OV-3, procedures for exchanging information in frequently repeated interactions in its OV-6 and corresponding SV-10 products, what systems need to interface to effect those communication exchanges in its SV-1, what protocols are needed to effect those interfaces in its TV-1, etc. Hence, roles and responsibilities are delineated without ambiguity within the integrated governance architecture.

The integrated governance architecture can be used to coordinate priorities among and within the tiers, and then be translated from its architectural and systems engineering language into formats familiar to any non-architect; such as training materials, standing operating procedures (SOPs), instructions, job descriptions and task lists for people in the organizations that need to interact to make the governance architecture work. In the very act of constructing a governance architecture using DoDAF principles and guidelines, roles and responsibilities needed from each organizations involved will become glaringly clear (and perhaps hotly debated, but at least now the needs have been identified and can be explained). The following example is provided to illustrate how this activity can directly help enforce and implement policy and guidelines (which are presently captured in verbally written directives, instructions, memos, guidebooks, etc.). The DoDAF states that "Process owners are responsible for identifying and updating the data set that supports their process (JCIDS, Planning, Programming, Budgeting, and Execution (PPBE), Defense Acquisition System (DAS), PfM), as well as publishing those requirements so that architectures continue to provide correct information" (Volume I, p. 3-3, DoDAF, 2007). One may ask, "How, exactly, do they do this?" A DoDAF-compliant Governance Architecture that is decomposed through every tier of accountability will capture this and many other policy requirements, identifying precisely *who* these process owners are, *what* information is contained in the data set, *who* needs the information managed by the process owners, *how* the requirements and data are communicated, and *how* architectures are updated as a result.

6. Analysis of the Net-Centricity Concept

In the context of the DoD, net-centric is defined as "the ability to share information when it is needed, where it is needed, and with those who need it," and *net-centricity* is "an information superiority-enabled concept of operations that generates increased combat power by networking sensors, decision makers, and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization" (Volume II, Section 2.5, DoDAF, 2007). In a systems context, "Net-centric is a condition for services and information, their governance, and their performance and quality. Net-centric is focused on satisfying mission requirements through reusable and accessible packets of functionality that make data serviceable (visible, accessible, understandable, trusted, and interoperable) in the context of communications and transport in the Global Information Grid (GIG)" (Langford on Net-centric, 2007).

Net-centric warfare (NCW) is the application of this concept to link entities in the battlespace, and includes all DoD mission areas (Warfighting, Business, National Intelligence, and Enterprise Information Environment Management) (NCOW RM, Section 7.4). A Net-Centric Environment (NCE) is "a framework for full human and technical connectivity and interoperability that allows all DoD users and mission partners to share the information they need, when they need it, in a form they can understand and act on with confidence, and protects information from those who should not have it" (NCOW RM, Reference Model Glossary).

The foundation for the NCE is the Global Information Grid (GIG), which is the "globally interconnected, end-to-end set of information, capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel." Because of the DoD's shift towards net-centricity and the need to effectively develop and manage the GIG, architectures are required to consistently capture net-centric concepts. This consistent representation of net-centric concepts aligns with the goals of integrated and federated architectures discussed earlier (Volume II, Section 1.2.1, DoDAF, 2007).

The Net-Centric Operations and Warfare Reference Model (NCOW RM) describes key strategies for enabling DoD transformation to an NCE, and describes NCE capabilities, functions, services, and technologies. It is intended to be a tool to help capability developers, program managers and their technical staffs, information technology (IT) architects, program and budget planners, and program oversight authorities transform and operate in an NCE (Section 1.2, NCOW RM). The NCOW Reference Model is designed to support all DoD components in the execution of the key DoD decision making processes (i.e., JCIDS, PPBE and Defense Acquisition) (Section 6 of Introduction, NCOW RM, 2005). As discussed in Chapter II, adherence to the NCOW RM is directed in policy through the Net-Ready Key Performance Parameter (NR-KPP).

The NCOW Reference Model states that operations in the NCE are to be based on a comprehensive information capability that is "global, robust, survivable, maintainable, interoperable, secure, reliable, and user-driven" (Section 7.1 of Introduction). Characteristics of these operations include increased:

- *Operational reach*, defined as a gain in the ability to share information and NCE capabilities,
- *Operational richness*, defined as an expansion of the sources and forms of information and related expertise to support decisionmaking,
- *Operational agility*, defined as the ability to provide highly flexible, dynamic, and interoperable computing, communications, and data infrastructure, and to rapidly adapt information and IT to meet changing operational needs, and

- *Operational assurance*, defined as the assurance that the right information to accomplish assigned tasks is available when and where needed, trust that the information is correct, and trust that the infrastructure is available and protected.

The development, maintenance, and use of architecture data in an NCE increases the reliability and efficiency of key decisions. Maintenance and use of architecture data in a net-centric environment is described in the DoD Net-Centric Data Strategy (NCDS). Like governance, the NCDS is implemented through tiered accountability (Volume I, Section 4.2, DoDAF, 2007).

The NCDS applies to all data assets (i.e., system or application output files, databases, documents, or web pages) on the GIG, including architecture data. Architectural data assets include integrated architectures as well as individual architecture products produced and stored in architecture tools and data repositories. "Implementation of the NCDS throughout the DoD architecture community will enable architecture producers and end users to discover, share, understand, and use architecture data and products created and stored in independent architecting environments across the Department" (Volume III, Section 2, DoDAF, 2007).

Table 10 presents the DoD Net-Centric Data Goals of the NCDS. In an NCE, architecture owners are responsible for maintaining visibility, accessibility, understandability, interoperability, and trustworthiness of their architecture data and ensuring that processes are in place for discovering, linking, exchanging. and integrating their data with other relevant data in the NCE. Architecture owners are advised to use services for configuration management, using net-centric technical standards, cataloging and linking architectures for federation, and storing their architectures in repositories that enforce net-centric data goals and support federated search services (Volume I Section 4.2, DoDAF, 2007).

Goal	Description
Goals to increase Enterprise and community data over private user and system data	
Visible	Users and applications can discover the existence of data assets through catalogs, registries, and other search services. All data assets (intelligence, non-intelligence, raw, and processed) are advertised or "made visible" by providing metadata, which describes the asset.
Accessible	Users and applications post data to a "shared space." Posting data implies that (1) descriptive information about the asset (metadata) has been provided to a catalog that is visible to the Enterprise and (2) the data are stored such that users and applications in the Enterprise can access it. Data Assets are made available to any user or application except when limited by policy, regulation, or security.
Institutionalize	Data approaches are incorporated into Department processes and practices. The benefits of Enterprise and community data are recognized throughout the Department.
Goals to increase use of Enterprise and community data	
Understandable	Users and applications can comprehend the data, both structurally and semantically, and readily determine how the data may be used for their specific needs.
Trusted	Users and applications can determine and assess the authority of the source, because the pedigree, security level, and access control level of each data asset is known and available.
Interoperable	Many-to-many exchanges of data occur between systems, through interfaces that are sometimes predefined or sometimes anticipated. Metadata are available to allow mediation or translation of data between interfaces, as needed.
Responsive to User Needs	Perspectives of users, whether data consumers or data producers, are incorporated into data approaches via continual feedback to ensure satisfaction.

Table 10 DoD Net-Centric Data Goals (From: Table 2-1 in Volume III, DoDAF, 2007)

The DoD Architecture Registry System (DARS) is designed to provide an environment for the above-mentioned services to improve reliability and efficiency of architecture data sharing. DARS realizes NCDS goals by making authoritative reference data *visible* and *accessible* to all users by associating discovery metadata with reference data sets, providing a federated metadata search web service and providing services for loading, extracting, and managing versions of the reference data (Volume III, Sections 2.8 and 2.10.1, DoDAF, 2007). Metadata is "descriptive information about the meaning of other data or data processing services (e.g., web services)." In the context of architecture data assets, the metadata provides information about the content of an integrated architecture, individual architecture products, or about the use of data processing and analysis web services (Volume III, Section 2.3, DoDAF, 2007). DARS makes authoritative reference data *understandable* and *interoperable* via database conformance with the CADM eXtensible Markup Language (XML) schema. DARS makes reference data *trusted* by enabling identification of the source, authority, release or approval status, access control and quality aspects of the data; as well as providing a robust set of capabilities for enabling management of multiple product versions. DARS is *responsive to user needs* by providing a scalable, web-based capability that supports use and reuse of authoritative reference data sets and architecture products in DARS or in databases federated with DARS, to support capability assessment, gap analysis, portfolio management, systems engineering, facilities management, capital investment planning, and other management decisions (Volume III, Section 2.10, DoDAF, 2007).

For instance, recall the example of the UJTL and its corresponding authoritative source, the Joint Staff, presented in the previous sections. "The UJTL elements are available for export from DARS as a CADM XML record set. This record set can be used in any architecting tool environment to ensure that instances of process activities modeled in that tool environment are authoritative and will be consistent with process activities based on the same reference data in models created in other tool environments. This enables architecture data integration, since each independently developed model using the same reference data can be integrated via those common reference data elements" (Volume III, Section 2.8, DoDAF, 2007).

7. Net-Centricity Issues

There has been some difficulty in defining precise criteria that can be used to conclusively assess net-centricity. Presently, there is a compliance assessment of net-centric standards and strategies for the Net-Centric Domain (NCD) of the Warfighter Mission Area (WMA) being conducted by the Army CIO/G-6 (Net-Centric Assessment, 2007). The purpose of this assessment is to inform the WMA functional domains on the net-centric health of their portfolio. The draft assessment report noted that development of assessment criteria was difficult due to the present lack of definitive guidance and objective criteria. One of the underlying objectives of this assessment is to identify an approach to a more long-term Net-Centric compliance process.

The Net-Centric Checklist (OASD(NII) DCIO, 2004) was produced to assist program managers in understanding the net-centric attributes that their programs need to implement to move into the net-centric environment. The user completes the checklist by answering a series of questions pertaining to compliance with net-centric strategies and design tenets. Example questions are "Describe how the system is aligned with the DoD Net-Centric Data Strategy," "Is all of the data that can and should be shared externally beyond the programmatic bounds of your system visible (i.e., advertised) to all potential consumers of the data?" and "Are Web services implemented by the program built using the following core standards?" While the latter question regarding standards is objective, the former two questions are rather subjective in nature, allowing for a wide variety of free text responses. From examining the questions in the Checklist, it becomes clear why the Army CIO/G-6 has had difficulty in conducting its net-centric assessment of the Net-Centric Domain of the Warfighter Mission Area. The Checklist Foreword states that the list will be updated as needed to reflect DoD standards, protocols and industry best business practices.

These are just a few examples illustrating that the boundaries and criteria defining net-centricity are still under development. Until the definition of and criteria associated with net-centricity matures, implementation is limited to existing documentation and guidance.

8. Recommendations

Given the above overview and synopsis of net-centricity, the following recommendations are made for incorporation into the AAIP as it evolves.

a. Develop appropriate EEAs, MOEs, and MOPs for net-centric compliance criteria.

In the context of DoD Architectures, the NCOW RM provides the following criteria for effective operations in the NCE (Section 3 of the How to Use chapter, NCOW RM, 2005):

- *End-to-End Connectivity* – Connectivity throughout the environment described and connectivity to the NCE
- *Service-Orientation* – the services it requires, uses, provides, and manages
- *Assured Information and Services* – how information and services are assured
- *Information and Services Sharing* – how information and services are shared
- *Collaboration and Collaborative Decision Making* – how collaboration and collaborative decision making occur

In addition to these general criteria for effective operations in the NCE, the following net-centric attributes are provided to further characterize net-centric operations and warfare (Section 7.5 of Introduction, NCOW RM, 2005):

- *Internet Protocol (IP)* – Data packets routed across networks, not switched via dedicated circuits
- *Secure and Available Communications* – Encrypted initially for core network; goal is edge-to-edge encryption and hardened against denial of service
- *Only Handle Information Once (OHIO*) – Data posted by authoritative sources and visible, available, usable to accelerate decision making
- *Post in Parallel* – Business process owners make their data available on the net as soon as it is created
- *Smart Pull (vice Smart Push)* – Applications encourage discovery; users can pull data directly from the net or use value-added discovery services
- *Data Centric* – Data separate from applications; applications "talk" to each other by posting data
- *Application Diversity* – Users can pull multiple applications to access the same data or choose same application (for example, for collaboration)

- *Assured Sharing* – Trusted accessibility to net resources (data, services, applications, people, collaborative environment, etc.)
- *Quality of Service* – Data timeliness, accuracy, completeness, integrity, and ease of use

More research on each of these criteria, and formulation of these general criteria and Net-Centric Checklist questions into appropriate EEAs, MOEs, and MOPs should be conducted to help assess compliance with net-centric concepts and to measure progress. This activity should be coordinated with the Army CIO/G-6's Net-Centric Strategies and Standards Compliance Assessment activities (Net-Centric Assessment, 2007).

b. <u>Create the Governance Architecture described earlier in this chapter using the NCOW Reference Model as a guide.</u>

Given that the NCOW RM is intended to be used as a guide for building net-centric Information Technology (IT) architectures, it follows that this reference model can also be used as a guide for building a net-centric Governance Architecture. Recall that the proposed Governance Architecture discussed earlier in this chapter is a DoDAF-compliant description of the interactions required among organizations, people and systems to build integrated architectures. It is recommended that this Governance Architecture be built in a net-centric environment designed to achieve the characteristics of operational reach, richness, agility and assurance introduced earlier, as well to achieve the NCDS goals of visibility, accessibility, understandability, trust, interoperability, and responsiveness to user needs. Establishing a culture of net-centric operations and behavior among the human architects will promote and facilitate the defining of net-centric criteria as well as the designing-in of net-centric principles and guidelines into the more complex architectures being built by the architects, because they will have first hand experience with implementing these principles and guidelines in simply communicating with their peers, superiors and subordinates as defined in the Governance Architecture.

The guidance provided in “The Reference Model and DoD Architectures” in the “How To Use the Reference Model” chapter of the NCOW RM provides a general description of how to apply the reference model to the development of DoD architectures. Specifically, it describes:

- how to apply the Operational Element of the NCE, in which the architect selects activities organized and defined in the Operational Models that apply to the architecture, and incorporates and describes those activities in the architecture;
- how to apply service-oriented models and processes, in which the architect specifies and describes the service-oriented roles, service-oriented operations, services provided by the program, and applicable service contracts;
- how to apply the Systems and Services element of the NCE, in which the architect uses a Service Taxonomy and other information to identify and organize required services and align services with systems; and
- how to apply the Target Technical View (TTV), in which the architect identifies current and emerging standards and technologies considered essential to achieving net-centricity.

It is recommended that future work include the application of the NCOW RM to the Governance Architecture and other architectures developed using the AAIP. A useful context in which to describe this application would be to conduct a gap analysis between how the AAIP is used to govern, develop, and integrate architectures now versus how the AAIP would do so in a net-centric environment.

c. <u>Make it standard practice to use the DARS as a collaborative environment to access and work with authoritative reference data from federated databases.</u>

The DoDAF states that “at a minimum all architecture metadata should be registered in DARS to ensure effective architecture information sharing” (Volume I, Section 3.3.3, DoDAF, 2007). This minimum requirement, however does not enforce federation, merely that the architect to store metadata in the DARS directing users to the repository where the data is actually stored. The earlier recommendation to have Army Executive Architects make a concerted effort to federate their databases is therefore reiterated here, so that the DARS serves as a direct connection to the data (meeting *visibility* and *accessibility* requirements of the NCDS).

All architectures should be required to conform to the CADM XML schema used by DARS, so that architectures and architecture reference data is *understandable* and *interoperable*. To enhance understandability and interoperability of architecture data using commercial and government architecture tools, an Architecture Interoperability Program (AIP) is sponsored by OASD(NII) that assists tools developers in implementing the CADM XML specification. Specifications for interoperability with DARS are available in the AIP community in DARS (Volume III, Section 2.10.3, DoDAF, 2007).

The DARS should continue to be improved in *response to user needs* while remaining consistent with the concepts of architecture federation, tiered accountability, and net-centricity.

Finally, appropriate EEAs, MOEs and MOPs should be developed for the NCDS goals so that progress towards satisfying the goals can be measured.

The DARS should further be used by the Army Executive Architects and other component architects as a working collaborative environment for integrating and federating their architectures. DoDAF highlights that “The DARS provides a trusted environment for the sharing of architectural information. Using and contributing shared architectural information reduces cost, improves efficiency, and ensures reliability” (Volume I, Section 2.1.4, DoDAF, 2007). Furthermore, the DAG highlights the importance of developing a distributed collaborative environment accessible by all stakeholders. “A distributed collaborative environment will support authoritative information exchange and rapid refinement of the design or concept due to changing circumstances such as technological advancements and changing threats, tactics, or doctrine” (Section 4.5.7.1, DAG, 2006). The DAG goes on to discuss a process employing M&S to address capability needs in a collaborative environment. “When a needed capability is identified, M&S can be used in the collaborative environment to examine and explore alternatives and variations to proposed concepts. Rigorous examination, by all of the stakeholders, of proposed and alternative concepts applied through the effective use of M&S can help identify enabling technologies, constraints, costs, and associated risks. This rigor early in the concept refinement process is vital because the resulting decisions made in this early phase have repercussions throughout the system's life cycle that drive the ultimate life-cycle costs of the system (Section 4.5.7.1, DAG, 2006).

The use of reference lists and reference matrices, which are owned and maintained by their respective authoritative organizations as described in the section on Architecture Federation, maximally benefits the community when accessible and available in a collaborative net-centric environment such as the DARS. Architects should store and use reference lists and reference matrices in DARS to make maximum reuse of data that is common across multiple architectures. This practice significantly speeds the architecture development process since baseline material has already been developed. The architect's main development activities then consist of customizing the relationships among the data instance values, updating existing use cases and create new ones as needed using the detailed data already available. This increased reuse during the development process decreases the proportion of time *developing* architectures and increases the proportion of time *analyzing*, *improving* and *updating* them. As a result, more relevant and robust integrated architectures are available throughout the system or SoS's lifecycle for supporting major decision points as well as enabling Operations and Support phase quick-turn analyses with a data set that has been kept up to date throughout its lifecycle.

The architecture federation concept can be used in DARS to federate models and analysis capabilities, such as architecture certification tools, gap analysis tools, and simulation programs to enable collaborative improvement of the architectures and architecture data accessible via DARS. "Characteristics of a collaborative environment will entail models and simulations at multiple locations that are run and operated by subject matter experts and connected by wide area networks on an as needed basis. As changes are made to define a system that meets the needed capability, all stakeholders in the system's life cycle will have an active role in the changes being made" (Section 4.5.7.1, DAG, 2006). Using M&S early in the integrated architecture development process is most effective in a collaborative environment, since the architects would otherwise not have access to highly changeable OA, SA, and TA data. Consistent with the "Post in Parallel" net-centric characteristic, business process owners should make their data available via DARS as soon as it is created, rather than withholding draft data from the community until long after the community has the opportunity to influence and improve that data. By adopting a community wide culture of posting draft data for early modeling and analysis purposes, the concept of *draft* architectures and *final* architectures begins to disappear in favor of an *architecture continuum* that is constantly being optimized.

E. CURSORY ANALYSIS OF THE RESOURCE COORDINATION AND PRIORITIZATION SUB-PROCESS

Prior to concluding this chapter, it is worth performing a cursory analysis of the Resource Coordination and Prioritization sub-process[5]. This sub-process is a decomposition of the Main Process Activity 2, and depicts a Work Plan Prioritization process that iterates every fiscal year, concerning G6 AAIC coordination with G3/5/7 and Executive Architects in prioritizing customer requirements for the development of integrated architectures and resource allocation (Army CIO/G-6 AAIC, 2007). Of the steps in this sub-process, the step with the most potential for additional rigor is the step concerning actual Review, Prioritization and Resourcing of Integrated Architecture AV-1s. This step entails the collaborative review and prioritization of the AV-1s by a Prioritization Board consisting of representatives from G8, G6/AAIC, G3/5/7, Executive Architects and Other Architecture Producers; in accordance with Chief Architect's priorities and AAIC prioritization memorandum. The present core methodology used is as follows: (1) organize the proposed AV-1s and their associated funding

[5] A detailed analysis of the Resource Coordination and Prioritization sub-process, as well as the Integrated Architecture Certification sub-process, is identified as future work, as they are beyond the scope of the thesis.

requirements into bins according to the Chief Architect's priorities (e.g., Chief Architect Directed, Army and Joint Transformation, Enterprise Architecture, and Tools & Repositories); (2) have board members rate each AV-1 according to a set of defined and mutually understood criteria (units are either binary (0 or 1) or on a scale of 1 through 5 to add up to a maximum score of 10); (3) consolidate the scores of each board member with a "vote" into a common Excel workbook listing the AV-1s by bin; (4) sorting the AV-1s in each bin from highest to lowest score to show rank order of priority; and (5) allocating funds from the highest to the lowest rated AV-1. A cut line is drawn where the funds run to zero, and the results of the ranking are forwarded on as a recommendation to a Council of Colonels (CoC) for final assessment and prioritization. In both the FY06 and FY07 iterations of this process, some of the end results of this effort surprised the board. For example, some AV-1 that were, by all accounts, intuitively high in priority ended up ranking below AV-1s that were intuitively lower in priority. These incongruities are usually resolved during the CoC; however, there is a better way of conducting the AV-1 rating and ranking process, using the systems engineering analysis process presented in Chapter III. In this case, the EEA is "Which integrated architecture efforts should be resourced in FY*XX*?" The Measures of Merit are the criteria used to evaluate each AV-1 (step 2 of current prioritization methodology), a rigorous and proven evaluation technique is identified (such as a pair-wise comparison methodology to minimize intuitive incongruities[6]), the source data is the information provided in each of the AV-1s, and evaluation of alternatives is a further step not being currently done with analytical rigor, but can be done by constructing a model for the AV-1 ratings and rankings that allows "what if" excursions. Such a model would be extremely effective at the CoC to show, in real time during the meeting, different

[6] Pair-wise comparison is a method of comparing each to each. It is a Multi-attribute decision making (MADM) technique used to make a selection from a set of discrete alternatives. More involved methods using pair-wise comparison can account for uncertainty and decision maker preferences (e.g., Analytical Hierarchy Process and Utility Theory (Whitcomb, 2007)). In this context, each AV-1 would be compared with each other AV-1 in the same bin, assigning a *relative* importance on a scale that helps to quantify the degree to which the rater believes one AV-1 is more important than another (e.g., equally important, moderately more important, strongly more important, very strongly more important, or extremely more important).

alternatives, their impacts, and quantitative trade offs between resources and AV-1s. This model would ensure traceability of resourcing decisions to a robust, pre-defined process and removes ambiguity and doubt over the rigor with which the ranking of the AV-1s was determined.

F. SUMMARY OF BENEFITS TO THE ARCHITECTURE COMMUNITY

Implementing architecture federation, developing a "governance architecture," and conducting architecture development and integration in a collaborative net-centric environment will have many benefits to programs and components and up through the DoD Enterprise. These architectures can be reliably used as quality input data to measure cost; performance; interoperability; satisfaction of requirements; manpower and training; logistics, deployment, and asset allocation; schedule, and many other Measures of Merit (Volume III, Section 1.3, DoDAF, 2007). From these architectures, "task and process-activity staffing levels, technical standards such as communications protocols, network architectures, scenario information, and performance data, can all be input to M&S and analysis tools for performance measures computation." Using CADM structures for developing and maintaining measures of merit data provides the advantage of standardized data sets for use in M&S, analysis, and assessment tools, meaning the same data sets can be reused in various tools to support various types of analyses and enable these tools to evolve over time to provide a fuller set of measures required for decision support (Volume III, Section 1.3, DoDAF, 2007).

Benefits of using the DoDAF to create a governance architecture include the following:

- Clear delineation of architecture development roles and responsibilities in a tiered accountability framework
- Coordination of priorities among and within the tiers
- Provision of a means to document the architecture development process, and in so doing enable detailed analysis of the current architecture development process and discovery of efficiencies that can be gained in the process at each tier of accountability across the DoD Enterprise

- Use of a language familiar to architects (i.e., the DoDAF) to describe their own activities and process flows in developing architectures
- Instantiation of written policies into specific processes and exchanges, to show interrelationships among the policies as well as the dependency of successful integrated architectures on correct implementation of policies
- Extraction of training materials, SOPs, instruction manuals, policy updates, job descriptions, and task lists that can be used by non-DoDAF-speaking members of the DoD Enterprise who need to exchange information in support of integrated architecture development

Benefits of federating, validating and maintaining architectures in a net-centric environment (e.g., DARS) using a common data schema (e.g., CADM XML) include the following (Volume III, Sections 1.3, DoDAF, 2007):

- *Consistency* – CADM conformant data ensures consistency through the use of common data elements and taxonomies across levels of abstraction within the same product (up and down the hierarchies), as well as across products.
- *Data re-use and flexible partitioning* – Repeated use of architecture data by different teams for different purposes ("develop once, use many") provides efficiency, flexibility, and reduces the need for complex, costly, and sometimes infeasible reconciliations.
- *Inter-agency architecture data interoperability* – Interfaces to other architecture data repositories can be used to assess inter-organizational interoperability, gaps, or redundancy issues.
- *Ability to use multiple tools and perform ad hoc analyses* – Interfacing or federating of ad hoc reports, diagramming, executable modeling, and other modeling and simulation (M&S) tools to the data repository allows architecture developers and users to be unconstrained by the functionality of one tool.
- *Interfaces to other enterprise authoritative data sources* – Enables development of a direct interface to external authoritative data sources (e.g., the Universal Joint Task List (UJTL), DoD IT Standards Registry (DISR), IT Systems Registry list, organizations, occupational specialties, ships, aircraft, facilities, units, costing, and budget data) that currently requires manual inputting, parsing, or importing by each architecture developer).
- *Maintainability* – The "develop once, use many" heuristic and interfaces to authoritative data sources promote maintainability and validity of CADM conformant data.

- *Rapid Decision Support* – The integrated architecture data federation becomes an enterprise Decision Support System (DSS). CADM conformant data can be queried and analyzed, and reports can be generated for faster decision support and reduction of redundant data calls.
- *Integration with Enterprise Taxonomies* – Employing consistent taxonomies in the architecture data repository links knowledge management ontologies with Enterprise Architecture (EA).

Benefits of using reference lists and reference matrices in a federated architecture context include the following:

- Maximizes the amount of data that can be standardized and defined in a consolidated manner, since data common to more than one view is stored only once and referenced as many times as necessary (consistent with the "Only Handle Information Once (OHIO)" net-centric principle).
- Provides a baseline for customization for those mappings that need to be optimized for a specific architecture, and a data set on which to draw when developing the rule sets for the threaded products (e.g., OV-6 and SV-10 a/b/c products).
- Significantly reduces time and effort required to collect source data when initiating development of a new architecture.
- Captures relationships among technical, systems, and operational data, so that resulting OVs, SVs, and TVs are completely consistent and integrated with one another.
- Provides a means to adapt to rapidly changing doctrine, systems and parameters with efficiency and fidelity.
- Significantly reduces the turn-around time on updating highly detailed architecture products and the configurations of analysis tools linked to the reference data, enabling what-if drills.
- Allows exploration of impact of reference data updates (much of which is derived from doctrine) on all dependent architectures prior to giving authoritative approval for its use by the entire architecting community.
- Enables quick-turn studies to be performed while the architecture is still under development, and therefore allows analysis results to influence and improve the integrated architecture.

G. A NET-CENTRIC ARCHITECTURE INTEGRATION ENVIRONMENT

Using the concepts of architecture federation, architecture governance, and net-centric operations and warfare presented in this chapter, an NCOW RM-compliant; cross-organizational; AV/OV/SV/TV environment can be architected (as part of the proposed "governance architecture") and used by the Army and other components to integrate, analyze; and optimize their architectures in the context of the DoD Enterprise Architecture, the GIG. The federation concepts presented allow for organizations to use the tools that meet their specific needs, and federate the databases underlying those tools for integration and analysis purposes. A net-centric architecture integration environment would use DARS as an interface to access and integrate federated data sets, and extend the DARS with additional features that become possible in a net-centric, federated, and governed environment. Examples of such extensions include:

- *Analysis tools.* Federated analysis tools that can process CADM XML data sets can provide services to the architecture community by running standardized reports and analyses on the data. These tools can render system-of-systems OVs, SVs, TVs and user-defined, non-standard views on federated sets of architecture data; return reports to assist with data quality analyses such as architecture integration certification and gap analyses; or potentially include more complex functionality such as running simulations on federated models using scenario or configuration variants specified by the user.
- *Architecture feedback mechanisms*. Such mechanisms would help architects to collaboratively improve their architectures in the context of the larger system of systems. A system architect can recommend changes to the operational architecture, a technical architect can recommend changes in the system architecture, etc.
- *Introduction of architecture data wikis*. The notion behind a wiki (standing for "What I Know Is…") is to allow anyone to modify the data content, drawing on the knowledge of all users of the data. While presented here as an idea, a fuller analysis needs to be done to take advantage of the benefits of using a wiki to capture otherwise unstated knowledge of the users, while at the same time maintaining a set of authoritative reference data.

The successful implementation of a net-centric architecture integration environment as describe above would provide a rich and agile data foundation for systems engineering and SoSE using the systems engineering analysis process described in Chapter III, and should be developed to provide architects with the information and capabilities required to optimize the DoD Enterprise

Architecture as a whole. Consistent with the principle of tiered accountability, each organization would be able to optimize their own systems with full knowledge of the other systems (and their constraints) they need to work with in the DoD Enterprise System of Systems. The information presented in this chapter can be used to define the design criteria for such an environment. An implementation plan is presently under development for FY08 and FY09 at the Army Systems Engineering Office.

H. CHAPTER SUMMARY

This chapter described and analyzed key portions of the Army Architecture Integration Process (AAIP) in the context of the information presented in Chapters I through III, as well as additional research on the concepts of architecture federation, architecture governance; and net-centricity. Although the process that was analyzed in detail is Army-specific, the recommendations for the AAIP as it evolves are applicable in any program, component, mission area or enterprise-level context. Although this chapter details important aspects of significant concepts that enable architecture integration, it was not intended for this chapter to be an all-encompassing treatment of the concepts presented. Rather, aspects of these concepts were highlighted in order to enable the AAIP and other like processes throughout the enterprise to be developed in more detail and to support conclusions regarding the premise of this thesis. The information in this chapter can be used to define the design criteria for a net-centric architecture integration environment that can be used by the Army and other DoD components to integrate, analyze and optimize their architectures in the context of the overall DoD Enterprise Architecture.

V. CONCLUSIONS AND FUTURE WORK

A. INTRODUCTION

This chapter presents the conclusions, recommendations, and future work generated from completing this thesis. Section B discusses how this thesis addressed the research questions presented in Chapter I. Section C discusses general conclusions regarding the premise of this thesis. Section D summarizes the recommendations generated as a result of completing the research and analysis for this thesis. Section E summarizes potential areas for future work identified during the course of the thesis. Section F summarizes the chapter.

B. DISCUSSION OF RESEARCH QUESTIONS

The research questions described in Chapter I were developed to provide focus areas for the thesis and to shape the research and subsequent analysis of the data collected. The author found that the research and analysis conducted over the course of this thesis met or exceeded the objectives set forth in the three original research questions. Each research question corresponded well with the subjects of Chapters II, III and IV, respectively. The methodology presented in Chapter I, Section F was successfully used to address the research questions.

1. What do DoD Policy and Guidance State about the Need for Integrated Architectures?

This research question set an objective to review DoD policies, directives, instructions, manuals and guides for pertinence to integrated architectures and extracts highlights of guidance on their purpose and use.

The information provided in Chapter II discusses in detail the needs for and directives to develop integrated architectures in DoD, the architecture framework used for relating architectural data, features and characteristics of integrated architectures, and various uses for integrated architectures referenced throughout the literature. In addition to being mandated by federal law, architectures serve "to support strategic planning, transformation, and various types of analyses (i.e., gap, impact, risk) and the decisions made during each of those processes" (Volume I, Section 3.1, DoDAF, 2007). The takeaway from the detailed description of the uses of integrated architectures provided in Chapter II is that the ultimate purpose of architecture data is to inform decision-supporting analyses, which are aimed at improving the system described in the architecture, in an iterative way, throughout its entire lifecycle.

2. How Do Integrated Architectures Support Systems Engineering Analysis?

This research question set an objective to document the systems engineering analysis process used by the Army Systems Engineering Office, which has roots in DoD, industry, and academic publications, and to explore the relevance of integrated architectures to this process.

The information provided in Chapter III documents the quick reaction process used by the ASEO to conduct systems engineering, and further identifies existing correlations between this process and the DoDAF six-step architecture development process. Chapter III also describes how integrated architectures are used in the context of a systems engineering analysis process, and how that process may be applied to the JCIDS process and Defense Acquisition Process. A major finding is that the systems engineering analysis process and the DoDAF architecture development process should be brought together into one process so that integrated architectures become the source data used to conduct systems engineering analyses, and in turn, the systems engineering analysis results and conclusions are applied directly to the improvement of these integrated architectures to deliver higher quality products to the warfighter.

3. How Could the Architecture Development and Integration Process be Improved to Better Support Systems Engineering Analysis Needs?

This research question set an objective to investigate potential architecture development and integration process improvements in the context of the net-centric operations and warfare concept, in order to facilitate large-scale, high fidelity systems engineering analysis of the integrated architecture.

In order to give a relevant context to this analysis, Chapter IV summarizes and evaluates the Army Architecture Integration Process (AAIP) for potential improvements based on *three* concepts: architecture federation, governance architecture, and net-centric operations and warfare. The recommendations resulting from this chapter are based on research conducted for and documented in Chapters II through IV. Although the process that was analyzed in detail is Army-specific, the recommendations for the AAIP as it evolves are applicable in any program, component, mission area or enterprise-level context. The recommendations based on the research are aimed to enable large-scale, *collaborative*, high fidelity systems engineering analysis of integrated architectures. The information in Chapter IV can be used to define the design criteria for a net-centric architecture integration environment that can be used by the Army and other DoD components to integrate, analyze and optimize their architectures in the context of the overall DoD Enterprise Architecture.

C. CONCLUSIONS REGARDING THE THESIS PREMISE

The premise of this thesis is that integrated architectures have increased usefulness to the users of the systems they describe when they can be interactively and dynamically updated and used in conjunction with systems engineering analyses to enable systems optimization. In order to truly prove this premise as it is phrased, one needs to test it by developing an integrated architecture and providing its users with an environment in which they can interact with the data and dynamically update it, and assess the usefulness of the architecture in conjunction with systems engineering analyses and systems optimization. Although the research did not include the construction of such an experiment, the research found much evidence to support this premise throughout policies, guides, and processes. The following paragraphs summarize the conclusions founded on evidence presented throughout the thesis.

1. The DoDAF Takes a Data-Centric Approach

The data-centric approach of the DoDAF version 1.5 generally supports the premise of this thesis that integrated architectures have increased usefulness to the users of the systems they describe when they can be interactively and dynamically updated and used in conjunction with systems engineering analyses to enable systems optimization. Integrated architectures cannot be dynamically updated when they are only captured in static form, e.g., architecture products in portable document format (PDF), Microsoft PowerPoint, or Microsoft Word.

2. Models are Used to Represent Architecture Data

The DoDAF describes architecture products as representations of the data that are developed *in the course of modeling* relationships among related architecture components (Volume II, Section 1.2). The fact that the DoDAF describes architecture products in the context of modeling implies that the architecture products are not intended to be static, one-time use products, but must instead be dynamically updatable based on modeling results.

3. Architectural Data Sets are Required for Analysis and Improvement of Systems

As discussed in Chapters III and IV, the lack of access to an integrated architecture significantly lengthens the amount of time needed to collect, integrate, use, update, and *reuse* architectural data that is required for analysis throughout a system's life. Integrated architectures are required as foundational data sets for informing analysis questions, as well as for capturing improvements to the design identified as a direct result of iterative systems engineering analyses.

4. Architects Must be "Continuously Aware"

The DoDAF states that the architect must be *continuously aware* of the interrelationships in order to produce an architecture that is consistent across all four views, and to provide clear traceability from one view to another (Volume II, Section 2.4, DoDAF, 2007). The DoDAF also discusses the architecture views and their interrelationships providing “the basis for deriving measures such as interoperability or performance, and for measuring the impact of the values of these metrics on operational mission and task effectiveness” (Volume I, Section 1.4.1, DoDAF, 2007). If the architect is not continuously aware of the interrelationships, the views may get out of synch, and the architecture will have inconsistencies that potentially preclude the derivation of such measures. Such continuous awareness and insurance of consistency requires the means to dynamically update all parts of the architecture to provide a rigorous data set for systems engineering analyses.

5. Modeling & Simulation is Advised during the Acquisition Process

The Defense Acquisition Guidebook highlights the important role that M&S has in all aspects of the acquisition process, particularly when designing and developing a capability that is part of an SoS. It states that “today's systems and associated interactions are complex. M&S can assist the process by controlling the desired variables to provide a repeatable audit trail that can assist in the acquisition decision processes” (Section 4.5.7.5, DAG, 2006). The DAG further suggests that the Operations and Support phase may be considered the *first* phase of the acquisition lifecycle, since it is during this phase that new capability needs and requirements surface. Once an M&S capability for a system has been built up over the course of a lifecycle, the models may be reused as a baseline for programs entering the Concept Exploration phase, and additionally used as a representation of the system in other SoS M&S environments. Architecture configurations explored on previous iterations are captured and documented, and lessons already learned are consulted prior to repeating configurations that have already been found to be ineffective.

6. Increased Architecture Agility Is a DoDAF Guideline, a Benefit of Architecture Federation, and Enabled by Net-Centric Characteristics

Architecture agility is a DoDAF guideline for architecture development and integration. High agility is achieved with high modularity, reusability, and decomposability. Architecture descriptions should consist of related pieces that can be recombined with a minimal amount of tailoring to enable use for multiple purposes. An agile architecture provides the means for functioning in a dynamic environment (Volume I, Section 2.1.5, DoDAF, 2007). Architecture agility reduces the turn around time on systems engineering analyses by reducing the time needed to conduct what-if drills and alternate scenario excursions in search of optimal configurations.

Chapter IV notes that increased agility is specifically called out as a benefit of architecture federation. ”Users can search the GIG Architecture registry and find existing architecture content, significantly reducing the time and cost for new architecture development, fielding of a new capability, and gaining improved interoperability ‘out of the box.’ By using these building blocks, warfighters can swiftly adjust their architectures to meet changing business and mission needs” (Section 6, GIG Federation Strategy, 2007). Architecture agility, although highlighted as a benefit only to DoD Architects, also benefits warfighters (as noted above) equipped with the right tools, and DoD decision makers since the decisions often need to be made quickly, as in the cases where the ASEO quick reaction systems engineering analysis process is implemented to answer analysis questions.

The NCOW Reference Model calls out Operational Agility as a characteristic of operating in a net-centric environment (Section 7.1 of Introduction, NCOW RM, 2005). *Operational agility* is defined therein as the ability to provide highly flexible, dynamic, and interoperable computing, communications, and data infrastructure, and to rapidly adapt information and IT to meet changing operational needs. Operational agility, applied to architecture development, integration, and analysis environments, enables architecture agility.

7. Architectures Have a Temporal Dimension

The DoDAF states that architecture data supports program management and systems development by representing system concepts, design, and implementation *as they mature over time* (Volume I, Section 3.1, DoDAF, 2007). This statement implies that architecture data must have a temporal dimension, and the ability to dynamically change, adapt, and mature along with the real system that it describes. Such an architecture would be represented as a continuum of data and data interrelationships that is neither draft nor final. Rather, it would be a dynamically changeable model, of which snapshots can be taken to reference configuration versions and formally deliver architecture products, and describe configurations on which specific analyses were based. Once a complete baseline is established for a given architecture, the notions of “draft” and “final” architectures disappear. Nothing is ever draft, or final, just a representation of what the architecture looked like at a certain point in time. From this notion, a new premise emerges that as processes mature, the virtual environment in which IT architecture models and emulations reside can and should become virtually indistinguishable from the real architecture itself.

D. SUMMARY OF RECOMMENDATIONS

The following recommendations are made for further development of the Army Architecture Integration Process (AAIP) and DoD architecture development in general. Successful implementation of the recommendations summarized below will provide a case study for conclusively determining the degree of increased usefulness to the users of integrated architectures fitting the description in the premise. One may also conduct an investigation among specific architecture projects in government, commercial and academic institutions to determine the degree to which these recommendations are already implemented.

1. Develop Authoritative Reference Data

The concept of subject matter experts maintaining and providing authoritative reference data was found to be a common theme that runs through the three concepts of architecture federation, architecture governance and net-centricity.

With respect to federation, it is recommended that authoritative reference data be developed in preparation for implementation of the GIG Federation Strategy. The methodology for generating reference lists and matrices presented in Chapter IV should be further considered to enable maximum reuse of architecture data across the DoD enterprise. For the AAIP, it is recommended that this process be reviewed, improved and considered for adoption into the decomposition of Activity 3, Develop Integrated Architecture (OA, SA, TA), in the AAIP Integrated Architecture Development Process (Figure 13).

With respect to architecture governance, each organization in the DoD, at each tier of accountability, should be assigned the roles and responsibilities required for maintaining the reference data for which they are the subject matter experts, and which is needed by other organizations for constructing an integrated architecture. For the AAIP, it is recommended that publication and maintenance of pertinent reference data be defined and delegated to the appropriate authoritative sources.

With respect to net-centric operations and warfare, it is recommended that the authoritative reference data be shared and used in a net-centric environment, as described in Chapter IV. For the AAIP, it is recommended that Army Executive Architects make net-centric collaboration part of their process.

2. Develop Measures of Merit for Architectures

The DoD should expand and develop a set of measures such as those exemplified in Table 8 to measure architecture data quality, integrity and compliance with DoD policies and strategies. A set of measures can be customized for the high-level activities, capabilities, products, and services intended to facilitate implementation of federation strategy concepts to satisfy the GAO's recommendations that the DoD address the question of what milestones will be used to measure progress and results towards implementation of the BMA federated architecture strategy. Appropriate EEAs, MOEs, and MOPs for the net-centric compliance criteria in the current Net-Centric Checklist (OASD(NII) DCIO, 2004) should also be developed to help assess compliance with net-centric concepts and to measure progress. This activity should be coordinated with the Army CIO/G-6's Net-Centric Strategies and Standards Compliance Assessment activities (Net-Centric Assessment, 2007). Appropriate EEAs, MOEs and MOPs should also be developed for the Net-Centric Data Strategy (NCDS) goals so that progress towards satisfying these goals can be measured.

3. Conduct Architecture Quality Certification

It is recommended that a general Architecture Quality Certification be included in the AAIP in addition to Architecture Integration Certification, to encompass at a minimum all of the metrics outlined in Table 8, which are directly traceable to requirements in the DoDAF. A "certified integrated architecture" is, after all, limited in its utility unless it contains the necessary information for analysis, has "a purpose in mind," is "simple and straightforward," is "understandable among architecture users," and "agile."

4. Merge the ASEO Systems Engineering Analysis Process and DoDAF Architecture Development Process

As noted in Chapter III, a full evaluation of the two subject processes is required. The processes should be compared in detail, and the consequences of continuing to perform the processes independently of one another should be further evaluated. The processes should be combined, or rewritten to be entirely consistent, with one process dovetailing into the other, so that integrated architectures become the source data used to conduct systems engineering analyses, and in turn, the systems engineering analysis results and conclusions are applied directly to the improvement of these integrated architectures to deliver higher quality products to the warfighter.

5. Federate Architecture Databases and Tools

Army Executive Architects and other DoD architects should work on federating their databases using the DoDAF, the CADM and the DARS as described in Chapter IV.

6. Make the Use of DARS as a Collaborative Environment Standard Practice

The DARS should further be used by the Army Executive Architects and other component architects as a working collaborative environment for working with authoritative reference data, and for integrating and federating architectures, as discussed in detail in Chapter IV.

7. Develop a DoDAF-Compliant Integrated Governance Architecture

A governance architecture is and should be an integrated architecture in its own right, and should have an AV-1, AV-2, and corresponding OVs, SVs and TVs that describe the interactions among its constituent decision makers, other enterprise-level users, components, programs and the business systems used to effect governance. Use the integrated governance architecture to coordinate priorities among and within the tiers of accountability, and then translate it into formats familiar to non-architects such as training materials, standing operating procedures (SOPs), instructions, job descriptions and task lists for people in the organizations that need to interact to make the governance architecture work. A DoDAF-compliant Governance Architecture that is decomposed through every tier of accountability will capture policy requirements; identifying precisely *who* these process owners are, *what* information is contained in the data set, *who* needs the information managed by the process owners, *how* the requirements and data are communicated, and *how* architectures are updated as a result.

Apply the NCOW RM to the Governance Architecture and other architectures developed using the AAIP to enable multiple organizations to perform architecture development, integration and analysis in a coordinated manner. A useful context in which to describe this application would be to conduct a gap analysis between how the AAIP is used to govern, develop and integrate architectures now versus how the AAIP would do so in a net-centric environment.

8. Train the Workforce

Include training on the BMA federated architecture strategy, as well as the new GIG Federation Strategy and other policies, strategies and concepts presented in this thesis, in the architecture education curriculum being planned by OSD(NII) DCIO.

9. Use Systems Engineering and SoSE Processes and Techniques to Develop and Improve DoD Architectures

All organizations within DoD (including component and program owners of constituent systems) as well as those that interface with DoD (e.g., other federal agencies and multinational agencies) must collaborate to develop a successful SoS. Since the DoD Enterprise Architecture is an SoS, the tools of systems engineering, SoSE, and the systems engineering analysis process should be made available and their value communicated to these stakeholders in a coordinated, policy-driven way. A process based on the systems engineering analysis process presented in Chapter III should be instituted by the Army CIO/G-6 AAIC and the DoD at large for measuring and improving quality, usefulness, and integrity of architectures it oversees. The very same architecture and systems engineering techniques used to solve technical problems should be applied to manage business problems.

10. Implement a Net-Centric Architecture Integration Environment

Using the concepts of architecture federation, architecture governance and net-centric operations and warfare presented in Chapter IV, the Army and other DoD components should design and use an NCOW RM-compliant; cross-organizational; AV/OV/SV/TV environment (as part of the proposed "governance architecture") to integrate, analyze and optimize their architectures in the context of the DoD Enterprise Architecture, the GIG. A net-centric architecture integration environment would use the DARS as an interface to access and integrate federated data sets, and extend the DARS with additional features (discussed in Chapter IV, Section G) that become possible in a net-centric, federated, and governed environment.

E. FUTURE WORK

This section contains brief descriptions on areas for future research that were noted in the course of writing this thesis.

1. Conduct Further Development of the AAIP

The Army CIO/G-6 AAIC has good feedback mechanisms in place for continually refining its processes. For example, an After Action Review (AAR) was held on August 29, 2007 to collect feedback from all stakeholders involved in the AAIP's Resource Coordination and Prioritization sub-process. This sub-process has just concluded its second formal iteration using lessons learned from the first iteration. Candid suggestions were provided during the AAR by the stakeholders with the objective of improving the process on the next iteration. The recommendations in this thesis can be used to continue the development and improvement of the AAIP.

2. Document Challenges to the Successful Creation of Joint, SoS Architectures

A brief introduction to the challenges of developing architectures was provided in the Background Section of Chapter I. Using this thesis and other works as a foundation, these challenges can be expanded to explore specific hindrances of creating and managing architectures on the SoS scale, and ways to mitigate these hindrances. Some known and suspected factors to be considered include:

- Lack of common terms and definitions throughout the enterprise
- Amount of data to be managed and the various timeframes associated with all of that data
- Number of organizations and people across the enterprise who are working on architecture largely independently of one another
- Hesitancy among organizations to share data
- Difficulty in moving and translating that data for multiple uses
- Lack of institutionalized processes among program offices to ensure each system is designed to operate in harmony with others with which it will be deployed
- Multiple contradictory technical objectives under already stressful conditions and environments, such as information security levels, changes in authentication for the designated level of user trust, network accessibility, bandwidth, application performance, and mission completion times

3. Assess Impact of DoDAF 2.0 on Conclusions of This Thesis

The impact of the current work on DoDAF version 2.0 on the conclusions and recommendations of this thesis can be investigated. The goals of DoDAF 2.0 are to (1) address current DoDAF limitations, weaknesses, and deficiencies; (2) provide a data-centric approach to building, implementing, and using integrated architectures; (3) enable "federation" of architectures; (4) capture sufficient architectural detail for full DOTMLPF analysis; and (5) provide support for architecture-based analysis and assessments that link directly to mission outcomes and objectives for the DoD core processes (Volume I, Section 2.1, DoDAF, 2007).

4. Elaborate on the Need for Architecture Products Containing Rule Sets

Architects can construct sequences of events and rules involving the cause/effect relationships (e.g., OV-6a,b and SV-10a,b) that capture the conditions and alternative courses and ways in which missions can be conducted. Developing these rule sets are more difficult than developing specific threads (i.e., OV-6c and SV-10c), but they are invaluably useful for modeling because they represent many possible outcomes of the same mission. Developing these rule sets results in a more robust model and enables simulation and emulation to find optimal solutions under different scenarios and circumstances. A full elaboration on the need for the OV-6a,b and SV-10a,b products and a description of the benefits can be presented in a future paper.

5. Incorporate Examples with Each Step in the ASEO Systems Engineering Analysis Process

Since many people learn by example, it would be helpful to update the systems engineering analysis process presented in Chapter III by incorporating examples underneath each step to better illustrate the process as the steps are being explained. A simplistic example was presented in Chapter I in applying the process to thesis research and analysis, but a technical example illustrating how the process is used in executing an analysis using detailed MOEs and MOPs would be ideal.

6. Develop Additional Customizations of the Systems Engineering Analysis Process

Throughout the thesis, several examples were provided on how the quick-reaction ASEO Systems Engineering Analysis Process may be customized for specific applications. One customization can be done for DoD acquisition programs to follow and iterate through their lifecycles, as mentioned in Chapter III Section D. Another customization can be done for the Army CIO/G-6 AAIC's Army Architecture Integration Process (AAIP), using the "features of integrated architectures" presented in Chapter II and the example EEAs, MOEs and MOPs in Table 8 for use in analyzing the quality and integrity of architectures produced. A third customization can be developed for the Resource Coordination and Prioritization Sub-Process of the AAIP to rate and rank proposed architecture development efforts, as discussed in Chapter IV, Section E.

7. Elaborate on Types of Analysis Questions

A broader sampling of the types of analysis questions that can be addressed by the analysis process presented in Chapter III should be assembled, with example questions ranging across the lifecycle phases as well as Program-level through Enterprise-level. Questions applicable to Mission Areas and Domains should also be included.

8. Conduct a Comparison of Systems Engineering Analysis Processes

The systems engineering analysis process presented in Chapter III is the process used by the Army Systems Engineering Office. A cursory literature review on the subject did not turn up many well defined systems engineering analysis processes. Further investigation and a thorough comparison of systems engineering analysis processes throughout government, industry and academia should be undertaken.

9. Investigate the Current State of Authoritative Reference Lists

Peripheral research indicates that the Joint community is already engaged in the development of sets of authoritative reference lists. This work can be investigated and summarized for the architectural community so that more architects and their leadership are aware of the progress of activities, so that their work can be used (and evaluated in constructive feedback) as soon as available.

10. Compare Specific Architecture Development Methodologies

There are many architecture development methodologies, both tool-dependent and tool-independent, for generating architecture views. One such methodology (concerning the creation and customization of reference lists and reference matrices) was proposed in Chapter IV. Architecture development methodology is an important consideration, since the products that result from one methodology may be different from products that result from another. Structured, object-oriented, activity-based, and architecture specification model methodologies are implemented in a variety of architecture development tools. Architecture tools are generally methodology dependent, which often results in architecture data that are critical for analysis using those methodologies, but are not readily aligned with the current DoDAF view set or CADM specification. The result is that some tools and methodologies will be challenged in meeting the objectives of DoDAF and CADM conformance (Volume III, Section 1.2, DoDAF, 2007). If different methodologies are to be used to generate products for the same integrated architecture, it must be proven that those methodologies result in consistent outputs. A good comparison will use the same input data to generate the same architecture product views, and then conduct an error analysis on the results.

11. Create Architecture Tool Requirements Checklists for Functioning in a Federated Environment

Conduct a detailed study on architecture development, integration and analysis requirements to determine essential elements that are required of architecture development and analysis tools. A checklist or set of EEAs, MOEs and MOPs can be developed and used to evaluate and compare vendor tools for architecture development, integration, and analysis.

12. Replicate a Real Architecture in a Virtual Environment

As suggested above, processes and tools are maturing to the point where the virtual environment in which IT architecture models and emulations reside can become virtually indistinguishable from the real architecture itself. Work in this area should be explored and summarized in the context of its relevancy to the Army and the DoD Enterprise.

F. CHAPTER SUMMARY

This chapter presented the conclusions, recommendations and future work generated from completing this thesis.

APPENDIX. DODAF V1.5 ARCHITECTURE PRODUCTS QUICK REFERENCE

DoDAF Volume I, Table 1-4: DoDAF v1.5 Architecture Products

Applicable View	Framework Product	Framework Product Name	Net-Centric Extension	General Description
All View	**AV-1**	Overview and Summary Information	✓	Scope, purpose, intended users, environment depicted, analytical findings
All View	**AV-2**	Integrated Dictionary	✓	Architecture data repository with definitions of all terms used in all products
Operational	**OV-1**	High-Level Operational Concept Graphic	✓	High-level graphical/textual description of operational concept
Operational	**OV-2**	Operational Node Connectivity Description	✓	Operational nodes, connectivity, and information exchange need lines between nodes
Operational	**OV-3**	Operational Information Exchange Matrix	✓	Information exchanged between nodes and the relevant attributes of that exchange
Operational	**OV-4**	Organizational Relationships Chart	✓	Organizational, role, or other relationships among organizations
Operational	**OV-5**	Operational Activity Model	✓	Capabilities, operational activities, relationships among activities, inputs, and outputs; overlays can show cost, performing nodes, or other pertinent information
Operational	**OV-6a**	Operational Rules Model	✓	One of three products used to describe operational activity—identifies business rules that constrain operation
Operational	**OV-6b**	Operational State Transition Description	✓	One of three products used to describe operational activity—identifies business process responses to events
Operational	**OV-6c**	Operational Event-Trace Description	✓	One of three products used to describe operational activity—traces actions in a scenario or sequence of events
Operational	**OV-7**	Logical Data Model	✓	Documentation of the system data requirements and structural business process rules of the Operational View
Systems and Services	**SV-1**	Systems Interface Description Services Interface Description	✓	Identification of systems nodes, systems, system items, services, and service items and their interconnections, within and between nodes
Systems and Services	**SV-2**	Systems Communications Description Services Communications Description	✓	Systems nodes, systems, system items, services, and service items and their related communications lay-downs

- Continued on Next Page -

DoDAF Volume I, Table 1-4: DoDAF v1.5 Architecture Products (Continued)

Applicable View	Framework Product	Framework Product Name	Net-Centric Extension	General Description
Systems and Services	**SV-3**	Systems-Systems Matrix Services-Systems Matrix Services-Services Matrix	✓	Relationships among systems and services in a given architecture; can be designed to show relationships of interest, e.g., system-type interfaces, planned vs. existing interfaces, etc.
Systems and Services	**SV-4a**	Systems Functionality Description		Functions performed by systems and the system data flows among system functions
Systems and Services	**SV-4b**	Services Functionality Description	✓	Functions performed by services and the service data flow among service functions
Systems and Services	**SV-5a**	Operational Activity to Systems Function Traceability Matrix		Mapping of system functions back to operational activities
Systems and Services	**SV-5b**	Operational Activity to Systems Traceability Matrix		Mapping of systems back to capabilities or operational activities
Systems and Services	**SV-5c**	Operational Activity to Services Traceability Matrix	✓	Mapping of services back to operational activities
Systems and Services	**SV-6**	Systems Data Exchange Matrix Services Data Exchange Matrix	✓	Provides details of system or service data elements being exchanged between systems or services and the attributes of that exchange
Systems and Services	**SV-7**	Systems Performance Parameters Matrix Services Performance Parameters Matrix	✓	Performance characteristics of Systems and Services View elements for the appropriate time frame(s)
Systems and Services	**SV-8**	Systems Evolution Description Services Evolution Description	✓	Planned incremental steps toward migrating a suite of systems or services to a more efficient suite, or toward evolving a current system to a future implementation
Systems and Services	**SV-9**	Systems Technology Forecast Services Technology Forecast	✓	Emerging technologies and software/hardware products that are expected to be available in a given set of time frames and that will affect future development of the architecture
Systems and Services	**SV-10a**	Systems Rules Model Services Rules Model	✓	One of three products used to describe system and service functionality—identifies constraints that are imposed on systems/services functionality due to some aspect of systems design or implementation
Systems and Services	**SV-10b**	Systems State Transition Description Services State Transition Description	✓	One of three products used to describe system and service functionality—identifies responses of a system/service to events
Systems and Services	**SV-10c**	Systems Event-Trace Description Services Event-Trace Description	✓	One of three products used to describe system or service functionality—identifies system/service-specific refinements of critical sequences of events described in the Operational View
Systems and Services	**SV-11**	Physical Schema	✓	Physical implementation of the Logical Data Model entities, e.g., message formats, file structures, physical schema
Technical Standards	**TV-1**	Technical Standards Profile	✓	Listing of standards that apply to Systems and Services View elements in a given architecture
Technical Standards	**TV-2**	Technical Standards Forecast		Description of emerging standards and potential impact on current Systems and Services View elements, within a set of time frames

LIST OF REFERENCES

Army CIO/G-6 AAIC (2007). *Draft integrated architecture development process v0.29.* Unpublished manuscript.

Blanchard & Fabrycky (2006). *Systems Engineering and Analysis.* 4th Edition. Prentice Hall International Series in Industrial and Systems Engineering.

CADM (2007). *Technical Specifications for the Core Architecture Data Model (CADM) version 1.5*. Retrieved September 7, 2007, from https://dars1.army.mil.

CJCSI 3010.02 Series (2007). “Joint Operations Concepts Development Process (JOPSC-DP).” Retrieved September 8, 2007, from http://www.dtic.mil/cjcs_directives/cjcs/instructions.htm.

CJCSI 3170.01F (2007). "Joint Capabilities Integration and Development System.” Retrieved June 14, 2007, from http://www.dtic.mil/cjcs_directives/.

CJCSI 3470.01 Series (2005). “Rapid Validation and Resourcing of Joint Urgent Operational Needs (JUONS) in the Year of Execution.” Retrieved September 7, 2007, from http://www.dtic.mil/cjcs_directives/cjcs/instructions.htm.

CJCSI 6212.01D (2006). "Interoperability and Supportability of Information Technology and National Security Systems.” Retrieved June 14, 2007, from http://www.dtic.mil/cjcs_directives/.

CJCSM 3170-01C (2007). "Operation of the Joint Capabilities Integration and Development System.” Retrieved June 14, 2007, from http://www.dtic.mil/cjcs_directives/.

DAG (2006). Defense Acquisition Guidebook. Defense Acquisition University. Retrieved on June 22, 2007 from https://akss.dau.mil/dag/.

Damashek (2007). Army CIO/G-6 Architecture Operations Network and Space (AONS), Email correspondence, August 16, 2007. *Subject: RE: Workshops on DoD Architecture Education*.

DoD M&S Master Plan (2006). *Department of Defense Acquisition Modeling and Simulation Master Plan*, Issued Under the Authority of the Systems Engineering Forum, Office of the Under Secretary of Defense (Acquisition, Technology and Logistics) Defense Systems.

DoDAF (2007). *DoD Architecture Framework version 1.5*. Retrieved July 15, 2007, from https://dars1.army.mil.

DoDD 2000.19E (2006). "Joint Improvised Explosive Device Defeat Organization (JIEDDO)." Retrieved September 7, 2007, from http://www.dtic.mil/whs/directives/corres/dir.html.

DoDD 4630.05 (2004). "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)." Retrieved June 14, 2007, from http://www.dtic.mil/whs/directives/.

DoDD 4630.8 (2004). "Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)." Retrieved June 14, 2007, from http://www.dtic.mil/whs/directives/.

DoDD 5000.1 (2003). "The Defense Acquisition System." Retrieved June 14, 2007, from http://www.dtic.mil/whs/directives/.

DoDD 8000.01 (2002). "Management of DoD Information Resources and Information Technology." Retrieved June 14, 2007, from http://www.dtic.mil/whs/directives/.

DoDD 8100.1 (2002). "Global Information Grid (GIG) Overarching Policy." Retrieved June 14, 2007, from http://www.dtic.mil/whs/directives/.

DoDD 8115.1 (2005). "Information Technology Portfolio Management." Retrieved June 14, 2007, from http://www.dtic.mil/whs/directives/.

DoDI 5000.2 (2003). "Operation of the Defense Acquisition System." Retrieved June 14, 2007, from http://www.dtic.mil/whs/directives/.

DoDI 8115.02 (2006). "Information Technology Portfolio Management Implementation." Retrieved June 14, 2007, from http://www.dtic.mil/whs/directives/.

DoD Risk Management Guide (2006). Risk Management Guide for DoD Acquisition, 6th Edition (Version 1.0). Department of Defense.

GAO-06-831 (2006). U.S. Government Accountability Office (GAO). *Enterprise architecture: Leadership remains key to establishing and leveraging architectures for organizational transformation* No. GAO-06-831) Retrieved September 7, 2007, from http://www.gao.gov/new.items/d06831.pdf.

GAO-07-451 (2007). U.S. Government Accountability Office (GAO). *Business systems modernization: Strategy for evolving DOD's business enterprise architecture offers a conceptual approach, but execution details are needed* No. GAO-07-451) Retrieved September 7, 2007, from http://www.gao.gov/new.items/d07451.pdf.

Giammarco et al. (2005). DEFENSE ACQUISITION UNIV ALEXANDRIA VA, Giammarco, K., Carlomusto, M., & Lock, J. D. *Development and analysis of integrated C4ISR architectures.* Retrieved June 14, 2007, from http://stinet.dtic.mil/.

GIG Federation Strategy (2007). Office of the Assistant Secretary of Defense. *Global Information Grid (GIG) Federation Strategy*. Retrieved August 29, 2007, from https://dars1.army.mil/.

Griffin (2005). NAVAL POSTGRADUATE SCHOOL MONTEREY CA, & Griffin, L. K. (2005). *Analysis and comparison of DoDAF and Zachman frameworks for use as the architecture for the united states coast guard's patrol costal (WPC).* Retrieved June 14, 2007, from http://stinet.dtic.mil/.

Guide to SoSE (2006). *Guide to Systems of Systems (SoS) Engineering: Considerations for Systems Engineering in a SoS Environment (Draft – September 5, 2006).* Department of Defense. Unpublished manuscript.

Heylighen, F. (2007). Dictionary of Cybernetics and Systems. Retrieved August 4, 2007, from http://pespmc1.vub.ac.be/asc/indexASC.html.

Hutchens, B. (2007). The Net Ready Key Performance Parameter. Retrieved July 26, 2007, from http://jitc.fhu.disa.mil/iop_conf/2007/downloads/jt_staff_nr_kpp_unclas.pdf.

Introduction to Defense Acquisition Management (2005). 7th Edition. Defense Acquisition University Press, Ft. Belvoir, VA.

IT PfM Team (2007). Office of the Secretary of Defense / Information Technology Portfolio Management Team. *IT PfM Oversight and Governance.*

Langford on Net-centric (2007). Naval Postgraduate School, Graduate School of Engineering and Applied Science, Department of Systems Engineering. Email correspondence, September 5, 2007. *Subject: "references."*

Langford on Systems Engineering (2007). Naval Postgraduate School, Graduate School of Engineering and Applied Science, Department of Systems Engineering. Email correspondence, August 14, 2007. *Subject: "Systems Engineering."*

NCOW RM (2005). Net-centric operations and warfare reference model version 1.1. [Electronic version]. Department of Defense.

NPS Graduate School of Information Sciences (2007). Naval Postgraduate School Operations Research Department. Retrieved August 11, 2007 from http://www.nps.navy.mil/or/index.htm.

OASD(NII) DCIO (2004). *Net centric checklist, version 2.1.3*.

SEP Preparation Guide (2006). *Systems Engineering Plan (SEP) Preparation Guide version 1.02.* Department of Defense.

Test & Evaluation Management Guide (2005). 5th Edition. Defense Acquisition University Press, Ft. Belvoir, VA.

Transformation Planning Guidance (2003). Department of Defense. Retrieved June 14, 2007, from http://stinet.dtic.mil/.

Whitcomb (2007). Naval Postgraduate School, Graduate School of Engineering and Applied Science, Department of Systems Engineering, & Whitcomb, C. *System Assessment lecture on multiple criteria decision making.* Unpublished manuscript.

BIBLIOGRAPHY

Air Force Inst. of Tech Wright-Patterson AFB, OH School of Engineering and Management, Beal, R. J., Hendrix, J. P., McMurray, G. P., & Stewart, W. C. (2005). *Executable architectures and their application to a geographically distributed air operations center* Retrieved June 14, 2007, from DTIC STINET database from http://stinet.dtic.mil/.

Bae Systems, Reston, VA, Dickerson, C. E., Peppers, S. R., Cordell, B., Fortunato, E. M., & Brady, B. T. (2005). *Architecture-based operations analysis: An extension of classical operations analysis* Retrieved June 14, 2007, from DTIC STINET database from http://stinet.dtic.mil/.

Bearing Point Inc., Mclean, VA, & McGreevy, P. (2006). *Aligning net-centric practice with net-centric technology: A way forward* Retrieved June 14, 2007, from DTIC STINET database from http://stinet.dtic.mil/.

Benjamin, D. C., Elliot, L. G., Harrison, G. A., Hutt, R., & Kern, H. S. (2005). Modeling and enhancing C4ISR with executable architectures. *Proceedings of 2005 Fall Simulation Interoperability Workshops*.

Carnegie-Mellon, Univ. Pittsburgh, PA Software Engineering Inst., Wood, W. G., & Cohen, S. (2003). *DoD experience with the C4ISR architecture framework* Retrieved June 14, 2007, from DTIC STINET database from http://stinet.dtic.mil/.

DoDD 8320.02, "Data Sharing in a Net-Centric Department of Defense." (2004). Retrieved June 14, 2007, from http://www.dtic.mil/whs/directives/.

DoDI 8110.1, "Multinational Information Sharing Networks Implementation." (2004). Retrieved June 14, 2007, from http://www.dtic.mil/whs/directives/.

DoDI 8260.01, "Support for Strategic Analysis." (2007). Retrieved June 14, 2007, from http://www.dtic.mil/whs/directives/.

DoDI 8260.2 (2003). "Implementation of Data Collection, Development, and Management for Strategic Analyses." Retrieved June 14, 2007, from http://www.dtic.mil/whs/directives/.

Engineering Management and Integration Inc. Herndon VA, & Clemens, N. (2004). *Using the C4ISR architectural framework as a tool for assigning management and technical responsibilities* Retrieved June 14, 2007, from DTIC STINET database from http://stinet.dtic.mil/.

Mitre Corp., Colorado Springs, CO, Beamer, R. A., Henning, P., & Cullen, R. (2006). *The USNORTHCOM integrated architecture: Developing and managing a capabilities-based architecture as a program to enhance the homeland defense and military assistance to civil authorities mission areas* No. XCNORTHCOM (XCNORTHCOM)) Retrieved June 14, 2007, from DTIC STINET database from http://stinet.dtic.mil/.

Mitre Corp., Colorado Springs, CO, Beckner, S. G., & Beamer, J.,Raymond A. (1999). *Structured systems evolution: Employing dynamic, executable architectures* Retrieved June 14, 2007, from DTIC STINET database from http://stinet.dtic.mil/.

Mitre Corp., Mclean, VA, Washington C3I DIV, Troche, C., Eiden, J.,Gerald F., & Potts, F. C. (2004). *Architecture development lessons-learned: A three-year retrospective* Retrieved June 14, 2007, from DTIC STINET database from http://stinet.dtic.mil/.

Mitre Corp., Mclean, VA, Pawlowski, I.,Thomas J., & Hoffman, K. C. (2005). *Applying multi-agency executable architectures to analyze a coastal security operation* Retrieved June 14, 2007, from DTIC STINET database from http://stinet.dtic.mil/,

Mitre Corp., Mclean, VA, & Sowell, P. K. (2006). *The C4ISR architecture framework: History, status, and plans for evolution* Retrieved June 14, 2007, from DTIC STINET database from http://stinet.dtic.mil/.

Mitre Corp., Eatontown, NJ, & Dimarogonas, J. (2004). A theoretical approach to C4ISR architectures. [Electronic version]. *Proceedings of Military Communications Conference, 2004. IEEE, 1*, 28-33. Retrieved June 14, 2007, from IEEE Xplore database.

Naval Postgraduate School Monterey, CA, & Caffall, D. S. (2003). *Conceptual framework approach for system-of-systems software developments* Retrieved June 14, 2007, from DTIC STINET database from http://stinet.dtic.mil/.

Naval Postgraduate School Monterey, CA, Ruiz, D. L., & Williams, R. E. (2000). *Examination of automated interoperability tools for DoD C4I systems* Retrieved June 14, 2007, from DTIC STINET database from http://stinet.dtic.mil/.

Naval Postgraduate School Monterey, CA, & Shaw, T. W. (2002). *A systems engineering design analysis of a U.S. army secure storage system* Retrieved June 14, 2007, from DTIC STINET database from http://stinet.dtic.mil/.

Northrop Grumman Information Technology Inc., Reston, VA Defense Missions SystemS, & Wostbrock, B. (2002). *Joint C4ISR architecture Planning/Analysis system (JCAPS)* Retrieved June 14, 2007, from DTIC STINET database from http://stinet.dtic.mil/.

Ring, S. J., Nicholson, D., Thilenius, J., & Harris, S. (2004). An activity-based methodology for development and analysis of integrated DoD architectures . *Proceedings of the 2004 Command and Control Research and Technology Symposium*.

Science Applications International Corp., Mclean, VA, Lau, Y., King, M., Okon, W. J., & Kye, D. (2005). *Architecture modeling approach for net-centric enterprise services (briefing charts)* Retrieved June 14, 2007, from DTIC STINET database from http://stinet.dtic.mil/.

Science Applications International Corp., Mclean, VA, Lau, Y., Okon, W. J., Kye, D., & King, M. (2005). *Architecture modeling approach for net-centric enterprise services* Retrieved June 14, 2007, from DTIC STINET database from http://stinet.dtic.mil/.

Space And Naval Warfare Systems Center North Charleston, SC, & Lenahan, J. (2005). *Are service oriented architectures the only valid architectural approach for the transformation to network centric warfare?* Retrieved June 14, 2007, from DTIC STINET database from http://stinet.dtic.mil/.

Space And Naval Warfare Systems Command, San Diego, CA, Byram, J. K., & Harris, J. P. (2002). *Developing and fielding information dominance* Retrieved June 14, 2007, from DTIC STINET database from http://stinet.dtic.mil/.

Stone, A., Scott, C., & Rahmani, S. (1993). On definition and use of systems engineering processes, methods and tools. [Electronic version]. *Aerospace Applications Conference,* 197-205. Retrieved June 14, 2007, from IEEE Xplore database.

Vitech Corp., Vienna, VA, & Reynolds, J. P. (2006). *Validating DoD architectures: The promise of systems engineering* Retrieved June 14, 2007, from DTIC STINET database from http://stinet.dtic.mil/.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Army Systems Engineering Office (ASEO)
   Space & Terrestrial Communications Directorate (S&TCD)
   Communications-Electronics Research, Development and Engineering Center (CERDEC)
   Ft. Monmouth, New Jersey

4. Army Architecture Integration Center (AAIC)
   Architecture, Operations, Networks and Space (AONS)
   Office of the Army Chief Information Officer/G-6
   Arlington, Virginia